SINGAPORE – ccNSO Members Meeting Day 2
Wednesday, March 26th 2014 – 09:00 to 15:30
ICANN – Singapore, Singapore

UNIDENTIFIED MALE: We'll give our colleagues a couple of minutes.

UNIDENTIFIED MALE: Okay, we're going to be starting in two to three minutes, I think.

BRYRON HOLLAND: If the respective presenters are here, we have one. The rest of you, if you could form an orderly line and proceed to the front, that would be appreciated. And while folks are getting organized, I just wanted to mention that somebody at the ccNSO cocktail party forgot their swag bag, and it has your important personal notes in it, which I promise I didn't read. Because the handwriting wasn't clear enough. Anyway, we do have it.

And I think we have almost a full house, so good morning everybody. Welcome to day two of the ccNSO meetings. We have, as usual, a jam-packed agenda. The first session on security is going to be chaired by Nigel.

NIGEL ROBERTS: Good morning. For those of you who don't know me, I'm Nigel Roberts from .gg, almost a ccNSO councilor. Luis, do you want to join us up at the front? I think that just leaves us with Andrei, and I think he's down last, there's no desperate rush.

This topic is on security and, without more adieu, Mr. Security is, I think, right at the extreme end, but I think I can see him. Patrick, would you like to start?

PATRICK FÄLTSTRÖM: Sure. Thank you, very much. I've been asked to give a brief update on some of the latest advisories that we have released from SSAC.

One thing that is important to remember when I go through this report is our charter. The charter of SSAC is to advise the ICANN community and board on matters relating to the security and integrity of the Internet's naming and address location systems. Some people think we only work with DNS. It has to do with anything related to security and integrity.

The reports that we have written lately are, of course, focused on DNS security. For example, 57, 59, 62, 63 and 64. But, we are also dealing with various abuse issues, and that is one of the reports I will mention, number 65 on denial of service attacks which, unfortunately, we see quite a large increase not only using the DNS but any kind of UDP-based protocol.

We're still looking at internationalized domain names and related issues, including trademark clearing house, for those of you who are interested in that. And then, of course, WHOIS where there is, unfortunately, a parallel session at the moment and that's why my vice-chair Jim Galvin is not here. And probably that's why some people who should be in this room is not here, either, because internationalized registration data is an important topic for you.

There are two reports that we published lately. Let's take number 64 first. This is an advisory on DNS Search List Processing. In SAC064, SSAC first of all examined how current operating systems and applications process search lists. We're looking at security and stability implications with some search list behaviors. We also proposed a [inaudible] to improve the search list processing.

First of all, what is search list processing? That is a feature that allows a user to enter a partial domain name in an application. The operating system will expand the name through entries in the search list.

For example, if you have a search list which is somedomain1.com, somedomain2.com and the user just types system in the browser, the browser will look up system.somedomain1.com, system.somedomain2.com, and system in some order, not in a specific order. That's one of the implications here. So types in one domain name, looks up three.

We had a look at this and we see that there are great varieties in how operating systems handle these issues, everything from not apply search lists at all, which you see at the top which is a mechanism we call never, to what you see at the end, that the browser application don't only apply search list, they also add, for example, www before the domain name, which is a behavior that we think is not very good at all. But for some weird reason, applications like browsers are adding www in front of domain names. That's not good.

The second thing we are looking at when we now know that there are these various behaviors, we look at the implications. We have been

looking more carefully both at query linkage and also various privacy issues, not only that DNS query itself might carry privacy information, but also we have been looking at what happens when the application actually tries to connect to whatever data it got in the response, the IP address got in response. We see there are many protocols which actually happily deliver e-mail, cookies and all different kinds of things to potentially the wrong host.

It could be intentional. It could be the objective to register certain domain names to be able to create honeypots that collect this privacy information.

Specifically, we have been looking also at applications that move between different environments. For example laptops and phones that move between home, office and a conference like this, and we have been looking at the different behavior and the different configuration that we recommend later for enterprises.

If we look at queries to the root zone, we have been studying this for a couple of years, as you know. We see that the number of queries for specifically the two top-level domains, home and corp, are extremely high and much higher than all the others. We also see that the number of queries for .home has increased dramatically and, for .corp, just a little bit.

If we look at this with a long arithmetic Y axis, you see that there others that also increased quite quickly. For example, ICE and a few others.

Regarding the actual more generic namespace collision issues, there is, as you might know, the JAS advisers report out for public comment and I urge all of you to have a look at that one and comment on it.

If we look at what is actually happening when someone types in, for example, www.corp, or uses www.corp, and you do have search list processing, this is one of the algorithms that is in use. The laptop or the user, the client side, is issuing a query for www.corp, as you see on line number one. On line number two, you see that what's happening is that it gets back an NXDomain, which means the domain name www.corp does not exist.

Then you have the search list added corp.example.com, so you have a query for www.corp.corp.example.com, NXDomain. Then it adds Chicago, www.corp.chicago.example.com, and it gets back that NXDomain for that, as well. Then, at the end, it adds example.com. You have it look at www.corp.example.com and you get back an IP address. This is a normal search list processing that you see in quite a large number of operating systems and whatnot.

Now, as you might understand if you look at the first line, you have a query for www.corp. So this search list processing works only as long as you get NXDomain responses for all of those queries except the last one. If .corp is allocated at a TLD and someone registered the domain name www, then the first query will actually return an IP address. And that is what creates the whole problem.

So we have a straw man proposal, which includes, first of all, that there should not be any automatically generated search lists. They should be

explicitly configured. This includes DHP servers that should have explicitly configured search lists, if search lists should be used at all. The best thing is, of course, to not use search lists.

Secondly, that unqualified single-label domain names should never be queried directly. This fits into the previous proposal that we had from SSAC that having A record, address records, at the apex of TLDs is something that we strongly not recommend. There are some TLDs, specifically ccTLDs, which actually do have A records at the zone apex, and that is absolutely not a good thing. We here recommend that clients stop to query for those.

Instead, if you have a single label, in that case, search list processing should be applied, and the single label should never be queried.

Alternatively, if there are some mutli-label domain name, search list processing should not take place, and by having this straw man proposal, you know directly when you have something that looks like a domain name whether search list processing should take place or not. This is a big change from what's happening today.

So in this report, we recommend that RFCs are strengthened and updated that specifically talk about this straw man proposal and take that into account and try to come up with a well-defined algorithm for search list processing. And also, once again, point out that the work that ICANN currently is ongoing regarding namespace collision, that it's really important that that program is continuing.

Let me now mention very quickly, because we are sort of running out of time, SSAC 65 on Denial of Service Attacks. This report is explicitly about

how DNS infrastructure and abuse, but as many people, including many people in this room know, at the moment, we have similar attacks using NTP. So this is sort of a generic problem for all protocols that don't use a three-way handshake which implies the protocol itself validate that there is a bi-directional path between the client and server. This is when you have this problem.

The underlying problem with these attacks is that at the ingress of ISPs network, specifically close to the edge, there is no source address validation. This is something that has been recommended in the IETF and also the SSAC already, in report number four, told and recommended strongly to the community to start using source address validation. That is not implemented yet and we really need to work together to resolve that.

We talk about Denial of Service Attacks which, today are more than 300 gigabits per second to name servers, NTP servers and such. So if you run DNS servers, you need to be able to keep, to be able to handle 300 gigabits per second of traffic.

This is an image that shows you an Adobe logo. This is really interesting because what we are trying to display here is a PDF document created by Adobe with a graph showing the flow of data. When you have a Denial of Service attack, you have to look at the document that is hopefully passed around to all of you.

What we are doing is that we are, once again, pointing out the various weaknesses and errors and problems we have in the currently deployed network that we need to do something about. For example, we do need

better cooperation between operators of Internet infrastructure and manufacturers to be able to take specific actions. There is, for example, recommendations that network operators must take immediate steps to prevent network address spoofing.

This is so incredibly important. Even though I don't like regulation, I start to be close to actually start talking to regulators and tell them they actually need to do something about this. This is the number one, largest problem.

Second largest problem is that we have recursive servers here and there on the Internet that still allow queries coming from anywhere on the planet. This is also not a good thing because it gives the ability to get reflection attacks. Specifically, it's pretty bad that when we find these recursive DNS servers in everything, in CPs, in home routers that manufacturers are selling, and they're default configured to be able to respond to queries from the global Internet.

The worst case I've seen was one mobile operator that bought from a vendor the modems for 3G, and they shipped 150,000 of these before they discovered that it was a recursive server in it. The modem was not field upgradable. The users, the buyers of the modems, had to a shop or, themselves, reflash the modems, and of course, users don't do that. So we have 150,000 modems just in one ISP and they don't know what to do about it because they don't know how to. They could turn them off, but of course that would make their customers unhappy. So vendors must be better when they are shipping things with default configuration.

There are some other recommendations that we can skip. Thank you.

NIGEL ROBERTS: Thank you, Patrik, that was very interesting and – dare I say it – entertaining. I've always found it very strange that certain browsers put things like .com in the end, as if to give priority to a particular TLD and others.

I don't see anybody at the microphone yet. I'm sure there are questions and I'd like to encourage everybody to use the microphone in the middle of the room. If there are any questions for Patrik, can you wave your hand please and come up to the microphone.

PATRIK FÄLTSTRÖM: I am really happy everybody understood everything I said and will immediately take actions together with me to make sure that all of the problems are resolved. See you on Tuesday.

NIGEL ROBERTS: Thank you very much, Patrik.

Next on the agenda, we have something very interesting, which is we all need who to contact. It's Cristian and Luis.

CRISTIAN HESSELMAN: While the slides are being loaded, my name is Cristian Hesselman. I'm with the .nl. This is Luis Espinoza, chair of the Contact Repository Implementation Working Group.

Here we go. Anyways, I will be talking about a survey we conducted back in December and the potential next steps based on that survey. So, Survey Results and Proposed Way Forward, that's the title of the presentation. Can I somehow switch slides? Oh, it's over there.

Okay. So first of all, some background on the history of the working group. The goal of the working group was to look into the implementation of a ccTLD contact repository. That's basically a service, or a system, if you will, that enables ccTLD operators to contact each other in case of serious or major incidents regarding the availability and integrity of the DNS or the registration systems that are being managed by the various ccTLDs. This included work on the technical requirements, but also on funding models and governance models.

The working group was basically bound by a couple of requirements, which was the non-binding relationship between ccTLDs and other entities, diversity policies and practices guiding ccTLDs, and a couple of technical requirements such as 24/7 availability.

The working group was basically set up after the incidence response working group finished, which was back in 2011, so we've been going on for quite some time. Next slide, please. The layout is a bit off, so please try to ignore that.

The survey that we conducted back in December of 2013, the motivation for doing it is that, in doing the work, we discovered that we often have difficulties conveying the added value of the service because we didn't have any real-world use cases or real-world scenarios.

Also, we discovered that the financial constraints that were put in place somewhat complicated the development and the operation of the service, and as a result, also the work that we conducted in the working group.

We also felt that that the potential added value of the service depended on the number of subscribers that would participate in the system. It would only work if a large number of ccTLDs would participate.

Our final motivation for conduction the survey was that the TLD landscape, had significantly changed since the working group was established back in 2011 somewhere. We have registries, high-value targets, and of course, we also have the new gTLDs.

So we felt it was necessary to check with the community, how they perceive the added value of the service and how they felt about things like the costs associated with it.

The audience that we targeted were people responsible for security and stability at their ccTLD. If you could go to the next slide, please. These are basically the results.

We received a total of 53 responses, which is pretty good for ccNSO survey; 26 of the respondents actually filled out the questionnaire completely. The top table is the one with the scores for all the respondents. The bottom table is the one for the respondents who filled out the questionnaire completely, so they filled out all questions.

The most important questions are the third and the fourth one. “How do you feel about the added value of the contact repository?” and

"Would you be willing to pay for the service in the form of a subscription fee?"

In both cases, it turned out that people perceived the added value of the service as pretty high, but there was, let's say, limited willingness to actually pay for the service. That's the main result of the survey. Could you go to the next slide, please?

A global ccTLD repository is still being considered as valuable for the community, the ccTLD community. We're seeing a strong perceived added value. People are actually also willing to participate in drafting a realistic use cases that would further underpin the added value of this service. And we also focus on the right types of incidents. That's one of the questions we also asked during the survey.

But the problematic thing is that there is a tension with the willingness to pay for the service. Next slide, please.

We thought about that for a while and then we came up with the following recommendation, which is to take a iterative approach and start out very simple with a secure mailing list, so at virtually no cost. Then iteratively expand the system based on the experiences that people would have with the secure mailing list. That would, for instance, allow for trust building within a community. It would also allow for aligning the perceived added value with the cost of the service.

We also recommend that, at the same time, to consider alternatives, such as a more regional approach maybe through CENTR or through LACTLD. Next slide, please.

So if we would, let's say, opt for a secure mailing list, then this is what it could look like. This is just an example. You could have a [Mailman] service hosted by a neutral party, such as [ISAC] or ICANN. For each ccTLD, you could have the people responsible for security and stability of that ccTLD on that mailing list and it could, for instance, be the CEO of the ccTLD who decides who gets on the mailing list. Basically, that would then give you a very rudimentary contact repository, basically the list of subscribers, plus a communications channel, which would be e-mail.

Then you would need a second or a new working group to set up a management list. Since this is pretty simple, we reckon this would be doable before the London ICANN meeting. Next slide, please.

If you look at the time line, I'm not sure if you guys can read it in the back, but what it says here is that the blue part on the left is that the activity of the current working group. We would basically write our proposal and our recommendation and send it to the council. Then a new working group, which is in green, would set up the secure mailing list, which would then run roughly from June up until a couple of months, and then in the second half of this year – so maybe after the meeting in Los Angeles – we could refine the use cases, refine the funding model, refine the governance model based on the experience that we got through the secure mailing list. So that's the iterative approach. Next slide, please.

So proposed short-term actions. First one is basically write our formal report and send it to the council, including our recommendations. That's something we plan to do at the end of April. Then close the CRI working

group and start a new working group to implement the recommendations. Next slide, please.

This slide basically is to ask you for your gut feeling right now. What do you think of this approach? What would be the room temperature? Maybe you could use your red, green and orange cards to flag what you think, or not.

NIGEL ROBERTS: Thank you, Cristian. Luis?

LUIS ESPINOZA: I'm the chair of this working group and I want to tell you a little something about this roadmap of this working group. This working group has been here for a long time. At some point, to be honest with you, we got stuck in some kind of [inaudible] cycle about what could be the ideal contact repository and have some offer to provide the cost of that because we never get offered to provide the real cost to maintain this kind of contact repository. Then we get stuck in some kind of cycle.

This illusion about the secure mailing list comes here to break a little bit this vicious cycle, to provide some output. But I think it is important at some point in the future to take again the full contact repository with all the future it was [expecting] from the beginning.

Then this will be a very good solution, I think. Cristian came with this solution to the working group and it's very practical. I know [inaudible] is practical. I don't know what happened with us in the past, but it is

important to have your feedback in this, if somebody wants to say something.

NIGEL ROBERTS: Thank you to both of them. Questions? Questions?

CRISTIAN HESSELMAN: Maybe a show of cards will help. Maybe we can ask the people to raise the red and green cards.

NIGEL ROBERTS: You all have your colored cards. I'd like to see who's in favor of this. I don't see anything except the green cards. That's good.

CRISTIAN HESSELMAN: Thank you.

NIGEL ROBERTS: Now some questions? No, I mean I want some questions. Seriously? Are we all still asleep from last night? Well, thank you, again, to both of you then.

Next, Peter? Can you go to the microphone, please?

PETER HOSEIN: Thank you for the update. You mentioned the funding model could be subscription fee model. Do you have any indication in what band we're talking?

CRISTIAN HESSELMAN: I don't have that information. Perhaps you do, about the cost?

PETER HOSEIN: When you were discussing the funding model, you were suggesting a subscription fee. Do you have indication of the size of that fee? Just to estimate for whether it would be feasible for smaller ccTLDs or not.

LUIS ESPINOZA: Yes, the reference we had in the past was [inaudible] that these contact emergency operator in Europe, I think. The cost is something around $1,000 per year per cc. It's something like that. But maybe for a well-organized cc, it's common sense, but for most of the smallest TLDs or ccTLDs, they don't have enough conscious about the importance of this contact repository. Maybe it is not feasible to pay that amount of money.

My personal opinion about that cost is it's too high because, in fact, the contact repository is a system based on some address book and the other part of the service is a contact center-like services. That part of the contact repository is very expensive because you need people to proof all the millions of phone, not only electronic media. That other

kind of media like phone or fax, that kind of thing. It's very expensive to have people doing calling.

NIGEL ROBERTS: Thank you, Luis. Bart, did you want to say something? You were up at the microphone. Bart? You were up at the microphone. Did you want to say something? Okay, fine.

Okay, thank you very much, indeed. Next we have Ryan. I think he's going to talk about digital identity and some things. Is that right?

RYAN TAN: Yes. Good morning. My name is Ryan. I'm from .sg. This morning, I'm going to share with you a very interesting scheme that we launched recently. It's called VerifiedID@SG. Basically, it's trying to mitigate identity theft in .sg registrations.

I'm sorry. I'm not good with the Mac. I'm sorry it's a bit weird, but I'll just continue. The scope of my presentation is first I'm going to tell you what problem we are facing and how we went about doing the solutioning, and then what was our plan. Eventually when we launched, what were the issues that we faced.

The problem. The problem is that because we allow real-time and online registration on names, you'll find that it's not very difficult to fake identity or perform identify theft. By itself, it's not a big issue, but the issue is that identify theft is often a precursor to other forms of abuses, like malicious domain, trojan horses, so on and so forth.

And what is even worse is, even if we manage to catch the guy who performed that bad act, he can get away scott free because we basically do not know who the guy is.

Of course, you can mitigate such problems. How we do that, you can investigate suspicious cases. You look at the domain registrations that come in every day, pick up suspicious cases and follow up on them, or you can act on complaints.

How serious is the situation in .sg? These we come to know of, there's only a couple of cases. But the main worry is those that we do not know. To be honest, we do not know how many of our domain names are registered to nobody. Essentially, we look at it. This is actually a time bomb for us. Can you imagine somebody coming up to us saying, “What do you mean you do not know who registered that domain name?” This is something I think happened in China a couple of years ago. We do not want that to happen in our country.

So what do we do? We have a couple of solutions. The best way, we think, is for the person to apply in person with a stack of documentary proof. Our company serves individual identity card numbers, passports and so on and so forth. But, it's not going to work for us. We know that the business owners suffer.

Then we thought of other ways, but whatever solution we come up with, it has to meet three criteria. Number one, we need to have positive identification of the registrant. We need to preserve the online and real-time nature of the registration, and the verification process needs to be very fast and very simple.

We thought, “Ah, Singapore has something called the SingPass system.” It stands for Singapore Personal Access. Pretty much anybody in Singapore or who lives or works here is issued a SingPass, and this is done by the Singapore government after they know who you are.

What it is essentially is a user name, which is your IC number, like your Social Security number, and the government usually issues you a password. It's not [inaudible] This SingPass has been in use in many resources currently, such as for buying a house, buying a car, applying for credit cards [inaudible] and so on and so forth.

We thought, maybe there's a way to marry SingPass with domain registry registrations. It works very well because currently all .sg registrations already require a Singapore local [inaudible] contacts, so we say maybe we could further require a named contact to have a SingPass ID. This main contact could authenticate himself by SingPass and then he can vouch for the identity of the registrant.

We put a few more factors into the verification process and we hope that it will mitigate the identify theft cases because the admin contact could be implicated if he helps a crook buy a domain name.

How it works is admin contact has got 21 days to perform their verification, otherwise we will suspend the domain name, meaning the name will cease to resolve on the Internet. And you want to be very careful. We send out very nagging e-mail reminders on a daily basis to everybody – the admin contact, the registrant, the registrar.

This is what you will see on the WHOIS immediately after registration but before verification. There is a new domain status known as the

VerifiedID@SG-pending. If the admin contact reacts to our e-mail, he locks on to our VerifyID portal, clicks on this button here to lock on into SingPass, enter SingPass ID, password. Clicks on "meet," and it goes to this particular page where the domain name is listed with all the registration details, but a tick on checkbox and click verify button, and that's it.

This is a very fast new step. Five-minute process. Success e-mails will be sent to the admin contact and the registrant. On WHOIS, you will see the status to VerifiedID@SG-Okay.

After many years of preparation, we finally launched a six-month trial last year in May. Then we [pray], because we are actually prepared for the domain name registrations to drop because some people may think this is too much. "This is too much trouble. I'd rather buy a .com instead." Interestingly, there were very few negative feedback. We had about three such feedback over, say, 10,000 domain names. And there was no drop in the volume. In fact, the volume rose.

We found that the admin contact, 75% of them actually could verify their domain names within 24 hours. They were very cooperative. And by the 21 days, 99% of them would have verified. What we particularly like is that the quality of the registrant actually improved. People actually bothered called to say, "Hey, my reseller put the wrong data to the system. How do I get about correcting those data?"

There were no suspected cases of identity theft or any cases during the six-month trial.

On the negative side, we have increased in the e-mail and phone queries. But that's pretty normal. We felt we can converted the scheme into a permanent scheme since November.

The summary. From before, we didn't know who the person was who registered the domain. Now we have a real person who can vouch for the identity of the registrant. With that, thank you for the time.

NIGEL ROBERTS: Thank you, Ryan. It's very interesting. I can see that it would be very effective in a country where you have an established SingPass type system and it's also the admin contact must be a person to whom that applies. I would be interested in other TLDs, how that might apply to them.

Have we got any questions? I'm sure we must have some. I can see one. Please make your way to the microphone.

STAFFAN JONSSON: Hi, Staffan Jonsson, .se. What about corporations? Do you sign as an individual or corporations, as well?

RYAN TAN: The admin contact needs to be a person. So he vouches that the registrant is the corporation.

STAFFAN JONSSON: So it's connected to an individual person when you sign for a company then.

RAYN TAN: Yes, that's right.

NIGEL ROBERTS: Thank you. Thank you, Staffan. Anymore? Yeah, please come up to the microphone.

STANFORD MINGS: Hi, good day. Stanford Mings at nic.vi. Can you go back to the post, to the slide where it shows you the information regarding the user to verify? Okay.

RYAN TAN: Should I go forward or backwards? This is the one.

STANFORD MINGS: To where they verify. To where it's verified.

RYAN TAN: Where it's verified. WHOIS. This one.

STANFORD MINGS: Okay, so you're only showing the status information. You aren't showing any information regarding the SingPass or anything like that?

RYAN TAN: You mean the SingPass ID within the admin contact details? We don't.

As a background to this, our WHOIS is one of a kind. We only show the name of the registrant, admin contact and technical contact. The only extra bits of information that we show is the technical contact's e-mail address so no other information is on the WHOIS.

STANFORD MINGS: Okay, so you have a relationship with the Singapore government to confirm that the SingPass is a legit number?

RYAN TAN: Not directly. The person who owns the SingPass – when he authenticates with a SingPass, we know that he's the owner of the SingPass, so we do have a direct link with the government in that sense. I'm not sure whether I answered the question correctly.

STANFORD MINGS: When you say you're verified, how do you verify? How do you know I didn't just come off the plane and give you a number, a pass? How do you know? How do you, as the ccTLD?

RYAN TAN: You have the pass and you have your own password. If you go to this authentication portal to lock in using your username and your password, I know that you own this username.

STANFORD MINGS: Okay, I guess I'm not understanding it. This username and password, is that something that is provided by the government? I'm assuming that's provided by the government.

RYAN TAN: Yes.

STANFORD MINGS: How do you confirm that's the correct password?

RYAN TAN: I'll go back the slides and show it to you. This window at the bottom, it is an authentication portal run by the SingPass, which is run by the government. I show him to this portal to lock in and the portal gives me an okay or not okay answer ,and if it's okay brings him to my portal.

STANFORD MINGS: Okay, I see it. Okay, thank you.

NIGEL ROBERTS: So actually, it's a little bit like when you're paying for something by credit card and you are taken verified by Visa or something like that, except it's run by the government and it tells you it's this person?

RYAN TAN: Yes, in a way.

STANFORD MINGS: Could you say it's almost like two-step authentication?

RYAN TAN: This is a username and password. So your question is is there another factor? No. At the moment, no, but I think the guys are looking at another second factor for authentication for this login.

STANFORD MINGS: Okay, thank you.

NIGEL ROBERTS: Any more questions, please? If not, thank you, Ryan.

Okay, we have two more presentations in this theme. Is Barry Brailey here from .nz? Please come up. Okay, when you're ready.

BARRY BRAILEY: Good morning and thank you for the opportunity to come here and speak today. I'm going to talk about an initiative I'm involved in called

the New Zealand Internet Task Force. I subtitled it “A bottom up approach to improving the cyber security posture of a country.”

Quickly, the program, I'm going to introduce with a little bit of background about New Zealand and some of the scene set of how the NZITF came into existence. The birth of a trust group, so to speak. I'll cover .nz's role in that, and it has been quite significant, and then I'll touch on the way we work and some of the working groups, initiatives we're working on currently for New Zealand. I'm happy to take questions during, if important, but otherwise questions and answers at the end.

I'm a security guy. I've done security for both the New Zealand and the U.K. government in different roles. I've also worked for a global engineering company as a security guy. I'm currently the manager of security policy for the .nz Domain Name Commission, and my other role, I suppose, is vice chair of the New Zealand Internet Task Force.

To cover it, the NZITF is a non-profit with the lofty mission of improving the cyber security posture of New Zealand. It's a collaborative effort based on mutual trust. We try to get active participation out of our membership. We can only actually do stuff with people volunteering their time and effort and goodwill towards achieving some of our outcomes.

A little bit about New Zealand. I'm sure that everyone's familiar here. So, New Zealand, otherwise known as Middle Earth – pretty famously known as Middle Earth, I suppose. We're located quite far down in the Southern hemisphere, kind of halfway between Australia and

Antarctica, which explains the weather patterns that we experience as well.

I'd like to do my plug for the New Zealand tourism board here. New Zealand is an excellent place for many reasons. We're pretty good at sport. We're a good place to make movies. We also have some fantastic scenery. Adrenaline sport capital of the world. We have lots of sheep. Pretty famous for sheep, and in fact, for our 4.4 million population of people, we have 32 million sheep, so seven each. And those are some pretty attractive ones, I thought, on the bottom left there.

You can't be brilliant at everything. In terms of cyber security approach – and I'll be honest, I worked for both of the organizations that I'm talking about here. The government's approach to cyber security has not been breathtaking or huge in its scale. Back in 2002, the government did establish the CCIP, which had some CERT-like functions, but it primarily focused on cyber security threats to critical infrastructure. It didn't go as far as it actually becoming a national CERT.

Then, to a great extent, despite some significant efforts by Internet NZ and .nz entities to try and get a national CERT off the ground, not a lot really happened in the top-down approach until 2011 when they published Cyber Security Strategy, probably the last of the developed countries to actually publish it. But, they published it. It's worth a read. It won't take you long.

Then, off the back of that, the CCIP was expanded slightly to become the national cyber security center. I was also involved in that. I'll be honest. There is some decent resource there, but the scope is still quite

narrow, so they're focused on services for government agencies, critical infrastructure and a few large companies. We're still missing that national piece at this stage.

There's been a bit of legislative change, which I'm not going to cover in this. But that takes us up to 2012, if you think about the security landscape that the world was in at this time. Back in 2002, this is when we were really seeing all the blaster and worms were becoming extremely popular and home users were really becoming super aware of what security meant.

And then the rise of hacking, or at least the notoriety of hacking came out with the [NASA] attacks and subsequent extradition case, etc. Then saw the Estonia, Georgia attacks around 2006, 2007. This is like DDOS on a national scale, suggestions of government involvement. Then the [inaudible] espionage networks started to be talked about around the Ghostnet stuff in 2007, 2008.

Then, of course, the sort of significant point for New Zealand in the creation of this was the Conficker worm and the millions and millions of infections that that saw. New Zealand was actually quite heavily affected by this. The ministry of health was offline for a number of days. Several thousands of dollars' worth of clean-up action. Then, several months later in an unrelated incident, a district health board also suffered a significant Conficker outbreak. Although not massive, both of those incidents did actually impact the delivery of patient care in the health system, which obviously should be alarm bells.

But off the back of that, there still wasn't that impetus from the top down to actually address things or improve how stuff was doing. Since then, we've seen this sort of almost ubiquitous problems with the likes of the Zeus and the SpyEye botnets that proliferate around the Internet. And then, Stuxnet in 2010. Obviously, there's been an interesting evolution of how security is viewed since then, but it's been a very busy decade just to that point.

Going back to around 2008-2009, one of the people who is still involved in the Internet Task Force was invited to go to what was then called the Botnet Taskforce. It has since evolved into the Digital Crimes Consortium, the DCC event. Mike attended this. He works for Telecom, one of our larger telcos and ISPs. He came back and he found this collaborative approach to security to be quite interesting. A few months later, the Cyber Storm II exercise was held in New Zealand. And again, there's some security professionals getting together, this collaboration, the discussing and spitballing ideas. They started to get the idea that this could be something that would actually work as an approach to security.

Then in the 2009 Conficker issue in the New Zealand efforts of the Conficker working group, that's where those kind of impromptu and operational relationships certainly started to pay dividends.

In 2008, the Botnet Task Force in New Zealand was established. Then, in 2009, we renamed it to the New Zealand Internet Task Force because the scope quickly got bigger than just the Botnet issues that we were seeing. Around 2009, we were starting to think about how we could

expand the membership and the things that we were going to focus on. This was sort of the organic birth of the organization.

At this point, I feel it's quite useful to mention the involvement of .nz in all of this. So the domain name commission, the New Zealand registry services and Internet NZ were very engaged in the Conficker working group and they were also there in at the ground level, so to speak, and engaged in the whole Botnet Task Force to New Zealand Internet Task Force. They even formalized their support early on in 2009. They were keen to give us administrative support whenever we needed it. They provided venues for meetings, etc.

Then once we got into formalization, they've also been active participants as members. They employ me and allow me to spend some of my day job working on this, which is also a useful participation. They still provide the financial administration and facilities for our banking, etc., as part of the support to the society.

We also use the NZITF to influence as a group how we deal with security matters internally. So if it's a bigger than group-like issue, we'll consider using NZITF consultation or getting it through the NZITF. We've adopted it as a most integral part of how we're going to do security as a group.

The early days, obviously it was a fairly small start. We were deliberately not very public in how we were going about it. In the first instance, it was kind of, “Well, I know two other guys who would be good. We should get them involved, as well.” That kind of shoulder tapping, slow growth to get enough people to actually start to achieve some positive outcomes.

We were lucky enough, both myself and my predecessor at CCIP were able to spend a bit of our time. So although there were government employees involved, it wasn't a top-down initiative from the government, if you know what I mean. But quite often there would be other security-related events and we tried to coordinate a side meeting or a bit of a discussion on the growth of NZITF around there.

Certainly in 2009-2010, we established a steering committee and moved forward. Then 2011, we formally incorporated as a society, which is a little bit unusual for some of the trust groups. Those of you in the room who are members of some of those mailing lists and trust groups will appreciate that a lot of them don't actually have a legal presence. But, in order to achieve some of the things that we wanted, we needed to be able to have a bank account, amongst other things. Actually have a flow of cash and having incorporation as a society made that a lot easier.

We introduced a very easy membership fee structure so independent individuals, $50 a year for membership gives us enough funding, and then we have a corporate funding structure were some corporates donate about $500 as their membership structure.

We also, in 2011, held our first public fanfare publicly advertised event, which was where we were lucky enough to get Bruce Schneier in Wellington. He was there for another event, actually. We hired a theater and we had 400 people in to listen to Bruce Schneier. So the population of Wellington is about 400,000. So 400 people with enough of an interest in IT and security to want to come and listen to Bruce Schneier for 40 mintues was pretty significant. We saw a hype in our membership as a result because, obviously, our profile suddenly raised.

That was useful in terms of getting the right people in to actually get some work done.

Obviously with that comes a board. The board's pretty well spread across this security community. We don't have board members who are from the exact same company. It's one of our requirements. So the membership companies are there. We've got a couple of the larger telcos and ISPs, government department, independent consultants, myself, one of the banks and then Price Waterhouse Cooper all represented through the different members of the board.

The reason the board actually compose and comprise the majority of the working committee stuff, as well, so a lot of the initiatives are driven directly from the board because of the way we operate.

We do still operate with a trust group-like approach. Members are nominated and vouched on. That we still find is useful because we want to have those frank and candid discussions which, in the security community, if people aren't prepared to exchange information, there's no real collaboration that you can achieve. The only way that we've come up with so far to maintain that level of trust is to stick to this nominating and vouching. It's not an entirely open society, but it is an incorporated society, nonetheless.

We also adopted the traffic light protocol, which is pretty well known in the CERT community and the security community. That just gives us a classification system for how we can exchange information. It's pretty easily understandable: red obviously being somewhat sensitive, amber

and green being easier. We use that internally in communications and also in face-to-face meetings.

We organize two to three face-to-face meetings a year and a two-day conference where we try to get some international speakers in. A significant part we lay on is training and working groups, which I'll touch on a little bit more now.

Talking through some of the things we've been able to achieve in the last four years or so, we're really keen to provide technical training. One of the problems with being a rather remote country in the world is there is not an easy and abundant supply of technical security training or trainers in New Zealand. And, what technical training there is in New Zealand can also be quite cost prohibitive we find, which doesn't help with the development of skill sets. We've been lucky enough to secure a lot of support from various organizations. We invariably don't end up paying a lot of these guys for their time for actually providing the training. We might lay on accommodation. Occasionally we cover travel. But we do rely on getting a lot of time from people for free. We organize them as and when we can secure someone who is of a suitable standard to talk.

Some of these course topics I'm showing here we've delivered multiple times and in different cities. I think in the last four years we've probably trained in the region of about 300 people in these different things. They're predominately hands-on technical type training, and we deliver it for anywhere from $150 to $500 or $600, New Zealand, for two days technical training, which is amazingly cheap for hands-on technical training. We offer those to the broader security community – or the

public, I should say – if we have space, but most of the time we're full by the time we make the offering to membership.

We've also supported various industry and community initiatives, and we continue to lend that support, including support back to things like [Net Whoey] and encouraging our membership to get involved in that New Zealand IGT type process. We've arranged a couple of graduate [inaudible] as well. So as membership, we've two or three of the higher education institutes are also members of the NZITF. We've had master's graduates who have done their master's on things like Botnet. I'm sorry, Botnet reverse engineering or honeynets. We've placed them in industry on [consignments], etc., which has helped transition them into successful jobs within New Zealand. We've also, both through manpower and financially-supported research initiatives and survey type activity, as well.

I'll touch on some of our ongoing work within New Zealand, just to give you an idea of some of the working groups or initiatives that we focus on. We identified a couple of years ago that there was a shortfall in standards-based security professionals and security testing is something organizations can spend a lot of money on.

We identified an organization out of the U.K. called CREST, Council of Registered Ethical Security Testers. They're a pretty high standard. This is mostly the pin testing, but they're also into the network forensics, as well. We haven't formally established this into NZITF. We worked with Australia, for instance. We've got a growing number of guys that achieved CREST certification. At this time, we haven't built the buyer demand where they're prepared to pay extra for security testing, but as

neighboring markets start to adopt it, we envision that it will. CREST is one of those things where we've just incubated the idea. We've got it to a point where, once the demand and conditions are right, we can probably just spin it off and establish it as an organization in its own right and NZITF can go to focusing on its normal business.

We also identified that a lot of organizations in New Zealand would benefit from greater involvement in readiness training or cyber-exercising. We've got an ongoing initiative to focus on that. Thus far we've focused on some communications checks and testing the readiness and procedures of some of our membership. We now enter some scenario discussions and deciding if we want to move this forward to actual exercise play.

Then, the other one that's turned into, I don't know if you're aware, in Australia a few years ago they launched what's called the ICODE, which is the voluntary security code of practice for ISPs. It was presented to NZITF by Internet NZ, actually, as something perhaps we could look at and give some thought to. It's “Do we need the ICODE in New Zealand?”

The question, obviously, was we don't really know what the problem is and the ICODE seems to be a solution to the problem. So we needed to understand more about the problem before we went to this. We now realized we need to get those data sources that would help us make an informed decision about the size of the problem in New Zealand.

There's a lot of data sets from people like Shadow Server that are publicly available to organizations. Providing you have a right or an ASN or something like that, they'll give you data that's relevant to you.

Through negotiation and agreement, they actually give us all of the Shadow Server data that's relevant to NZ, and we also have signed NDAs with some commercial entities. Obviously, I can't actually tell you who they are, which would help. But yes, we signed these NDAs and received other data feeds on malicious websites, malicious domains, other Botnet feeds. Even this week at this event, someone's offered me another feed of data that could be useful, including malware samples that perhaps some of our universities might be interested in.

We brought all that data in, really, with the intent in the first instance to measure the size of the problem, but then we're security practitioners, so we have to actually see things get fixed. We get alarmed when we see bad things, so in the short term, we had to go out and identify the appropriate teams in New Zealand that we could off push this data to and ensure that they would reach out to customers or ISPs and try and clean up some of those problems. So it's ended up in almost a slightly more operational place than we were originally intending.

But now we're just starting to get the feedback from those recipients on what they think the main problems are. We're already seeing that the ICODE or a version of it might help, but it's not just in the ISP space that it would need to be targeted. So an ongoing piece of work that could well sit with us for quite some time. But, the aggregation and dissemination of the data was an interesting activity in itself.

Then on the vulnerability disclosure initiative, I thought I'd talk through the examples. This was last year. We'll call him a researcher. It was someone who discovered what he felt was a significant flaw in the Ministry of Justice website. In my opinion not quite necessarily the

correct path, he actually reported this to the opposition party, so an MP from the opposition party was the person that he decided that he should highlight this problem to. So obviously, political opposition parties being what they were, they gave the government 24 hours' notice before going to the media. There was a bit of media furor around it. Then the justice minister comes out and makes that comment, which obviously sends a shiver through a lot of security researchers that they're perceived as being hackers by the government in the same vein as burglars.

Within the NZITF, we realized that this highlighted an issue that had been simmering for quite some time, probably. At the time, we perceived it that if you report a security vulnerability to a New Zealand website owner, you've got a 50-50 chance of reported to the police. The other 50% of the time you'll probably spend hours if not days trying to explain to them why it's a problem, and then they may or may not do something about it. So, whilst vulnerabilities are being observed and discovered in the course of people's work, the reality is that most security researchers are reluctant to even try and report them because of the pain and hassle that that can invoke.

Obviously this is well back into the NZITF's core business, I suppose. We realized we had to do better. The NCSC from Holland actually published an interesting set of guidelines which gave us a good working template for how a responsible disclosure proposal could work on a national level. We drafted up a document that we felt would work for New Zealand. We released that for public consultation towards the end of last year. We did a six-week public consultation on it. We also presented on it and did forum-based consultation at the open web applications

security project and Kiwi-con, which is a hacker conference in New Zealand.

That consultation and feedback has been taken back in and the working group is now working on the final version, which we'll probably make public around the middle of the year. We'll probably get that signed off on at the AGM to make sure that the membership is happy with it at that time.

What we're trying to do with this one is just improve the maturity and the approach to these vulnerabilities. New Zealand Registry Services actually got a really good example. If you're on their website, NZRS has already published their vulnerability report and policy, and they also, on their website, published the vulnerabilities that have been reported and they've mitigated, etc., etc., which gives the recognition to the reporting party, as well, that they've done the right thing. What we would like is for a significant wave of New Zealand websites and businesses to take that kind of approach as a good, mature example of how vulnerability disclosure should be handled from both sides.

That concludes my presentation on the New Zealand Internet Task Force. I'm happy to take questions.

NIGEL ROBERTS: Thank you, very much. That was very, very interesting, actually. Come on, there must be some questions. I see one. That's great. Maybe that's just the start. If you'd come up to the microphone, that would be great, and if you could give your affiliation, as well, please.

NEIL EL HIMAM: Neil El Himan from .id. I just have a question with regard to the scope of the c-CERT or the CERT of New Zealand. Does it only cover the .nz, or any other top-level domain?

BARRY BRAILEY: NCSC, NCIP type stuff, do you mean? Or NZITF?

The NZITF, it's for New Zealanders, so anyone, any entity in New Zealand could be a member. It's not related to .nz as the ccTLD. And likewise with government initiatives, as well. They're New Zealand and not related to ccTLD.

NIGEL ROBERTS: Peter, I think. Yeah, thank you.

PETER HOSEIN: You mentioned that you're making use of data feeds of security incidents. These are not just related to DNS, as such? They're overall security incidents?

BARRY BRAILEY: Yeah. So it's the general feeds around Botnet infection rates that have been geolocated to being in New Zealand. It's not security stuff pulled from the DNS. And also malware distribution websites that have been identified through other sources – again, not DNS-related. It's a feed that we think will help explain the picture on the size of the problem,

but also that invariably the feed hopefully will have something that we can push to someone else to try and get things cleaned up and improved so that we're keeping that hygiene and ongoing cleanliness of New Zealand Internet space.

PATRICK HOSEIN: That's obviously on a national level. The Centre Security working group is working on a security incident repository and I'm wondering if there are ways in which we can tie those two together or if there is at least some bridge between the two sets of information, but I'll ask the chair of the Security Working Group to get in contact with you.

BARRY BRAILEY: Excellent. Definitely. I look forward to it.

NIGEL ROBERTS: Can we encourage any more questions? Any more comments? No, I think that's it. Thank you very much, indeed. That was very interesting.

Okay, we seem to be doing fine for time. So, Andrei.

ANDREI KOLESNIKOV: Good morning. So, let me continue the saga which we started November of 2012, so it's been quite a lot of time since we started an interesting experiment with leading Russian companies, which ended up in very interesting results and a very effective mechanism, fighting

malware and other kinds of bad things in the Internet with national domain names.

Let me just remind you how this works. We have partners, which is leading Russian companies, including Kaspersky, Yandex, Rostelecom, to name a few. What we do, we have data feeds and a database of the malware. From the partner we get an initial list of the bad domains, assign a hash number to this domain name and combine requests from the registry, the other domain names which belong to this hash number. So without disclosing the actual registrant data, we send it back to the database, send it back to the initial domain center, the partner, and get a final list of the bad domain names in the center database.

So the other people and other companies who have access to this database, within a 24-hour cycle, are able to tag malicious domain names with a bad code and phishing.

Actually, this initiative started to find an efficient way to fight phishing. From many points of view, this is most hazardous thing in the Internet. Currently, we have this 24-hour cycle to effectively block bad domains.

What then happens, for example, the search engine, the Yandex, which is more than 80% of the market in Russia, of the search market, they check the bad URLs, the bad domain names in their search engine. So they are not displayed in a search result. Also, these domains are tagged in the Kaspersky database, which has more than 200 million installations all over the world. Also some of the domains going back through the root cert to other cert members and also Rostelecom, the largest

telecom provider, operator in Russia, also have a few tricks to certainly attack these domain names for their customer user-base.

Also, one of our partners, which is [inaudible] we call it the cyber police, was actually collecting the evidence and writing it up so it can be used in different legal forms against the bad guys in the Internet.

What do we have now? We have 1.2 million domain names tagged in the database and, since the beginning of this year, we had about 21,000 domain names in the database, including almost 9,000 malicious, also. There is categories here. Let me show it. There is something wrong with the screen. Yeah, like this.

So added up, 6,000 malware, about 1,000 of the phishing domain names and about 2,000 SPAM domain names. The most common use of the domain names, of course, is the malware. Different kinds of bad codes and [inaudible] and bad scripts on the sites. This is very common thing on the Internet. Because it's really hard to find the legal ways or go after every malicious resource with police, for example, this scheme, which works with .ru, really very efficient. Those resources are being isolated by our partners, and these partners cover basically 90% of all Internet users in Russia.

Okay, there's some graphs on second level and third level malware. Interesting that most of the phishing, malware and SPAM sources are in the second level. They are not necessarily in the third level and other levels of domain names. The majority of the database is about second-level domains.

Also, there is some good trend, because when we started, we started to actually collect the data so we can see the pattern of growth of the number of malicious domain names, but since we operate already more than a year, we can see a little positive trend that domain names being deleted from the domain name registry database because of no use.

So, let me go back to our partners and again repeat that, for example, Yandex is using this database for isolation of the search result. Kaspersky 200 million installations of [antivirus] software. .ru has more than 100 million users as an e-mail platform. Group IV is going after the criminals and Rostelecom is doing some tricks on their network to isolate the bad resources.

Also, the site, which is listed in the first slide. Hold on. We call it the Netescope. This site is actually the front end, which is available for the public. And anyone can check the domain name with .ru and .rf extension and get the history of this domain if it was included in the database of the bad resources. We plan to translate the site into English because we see a demand from abroad to check the domain names. And this is basically it. Just a shot of data of the whole initiative.

This is not the first time I'm talking about this initiative. This is just update that this cooperation with the leading companies in Russia is really bringing the results. So, thank you very much.

NIGEL ROBERTS: Thank you. Okay, specific questions now on the Netescope presentation from Andrei? Ah, we've got an eager.

NORM RITCHIE: Great. I love this. Norm Ritchie from the Secure Domain Foundation. This is very similar to what the Secure Domain Foundation is doing with all TLDs. It's not specific to any individuals.

Two things. One, we noticed domains and all TLDs. Happy to get those to you and add them to yours because we don't want to duplicate the efforts. I'll find a way of doing that.

On that, do you have an API to submit domains in, or is it a manual process?

ANDREI KOLESNIKOV: It's actually API. The number of our partners is limited. It's not open for everybody because there's a tricky situation. It's a non-commercial project and we don't want to compete with the guys who's actually involved in the security business. For example, the Group IV and Kaspersky. So we have to be really accurate in getting these connections done.

We basically have all the resources from their commercial instances. So we do have APIs for the partners. We have a predefined data format because we're getting all this data in a different format, so we have converters for the APIs.

Also, I forgot to say we plan to – it's actually will start very shortly, we'll upload the whole database of malicious domain names in .ru and .rf to

our registrars. And our registrars also have this API they can add the suspicious domain names so it can be checked through the database.

NORM RITCHIE: Okay. We have additional data that you may not have, so I'd like to figure a way of giving that to you so that it works for you. We can talk offline.

ANDREI KOLESNIKOV: Of course. We also work with some unlisted partners, and we're getting the feeds from various sources, of course, because it's increasing the quality of the database, of the resources. The more partners we have, the more quality it is. Thank you.

NIGEL ROBERTS: Roelof?

ROELOF MEYER: Roelof Meyer from .nl. Andrei, I didn't your slide with the circular graph. Could you show it again?

ANDREI KOLESNIKOV: This one?

ROELOF MEYER: Yep. Does it mean that you have 750,000?

ANDREI KOLESNIKOV: Yeah, 1.2 million tagged domain names. It's a history. That's the whole history, of course, since November 2012. It's a lot, I know.

ROELOF MEYER: Yeah. No, I thought that must be wrong. Thank you. And I'm not being cynical.

ANDREI KOLESNIKOV: No, that's the way it is.

NIGEL ROBERTS: Do we have anymore questions or comments? Yeah, please, come to the microphone.

UNIDENTIFIED MALE: Hi, my name is [John] from [inaudible] registry. I'm interested in your data because .ru is same as Indonesia. So many [inaudible] so is it possible that we have some cooperation so that we exchange these things with us?

ANDREI KOLESNIKOV: We actually thought about it, but there is a natural divide, and you know this divide. Because when we're talking about .ru and .rf domain names, we're talking about the Cyrillic sites, 95% of the sites used with this domain names are Cyrillic targeted in the local populations. The

phishing tricks targeted to Russians are specifically in Russian, so of course we can do the cooperation with the other countries, with the other languages, but there will be very, very short and minimal crossing between those web resources because the bad guys operate on a local market.

NIGEL ROBERTS: Stephen, you're on.

STEPHEN DEERHAKE: Stephen Deerhake, .as. Andrei, a quick question. If you have a domain in this list of miscreants and the registration is dropped for whatever reason and sometime down the road it gets re-registered, because it was once used, how do you guys – is there something special you do there? What's your assumption?

ANDREI KOLESNIKOV: We plan to launch a service called WHOWAS. And, you can basically, if you are registrant, of course you listed if – for example, you buy the domain on the secondary market, you interested that this domain should be white and clean, whatever. So it will be possible for the user to check the WHOWAS history and see the domain was involved in some kind of malicious activity.

NEIL EL HIMAM: Neil, .id. I'd just like to extend what my colleague has just said with the fact that some of the .rus used for malicious websites for phishings and

so on using other than the natural language that you have. So does your statuses include those languages or no?

ANDREI KOLESNIKOV: No, we work only with our domain names. We don't accept – for example, we get the data feed from the thirds around the world and we just cut off all resources which are not related to .ru and .rf. So international domains. We don't resource it.

NEIL EL HIMAM: So when we have problems, say for example, with .ru, we report it to you?

ANDREI KOLESNIKOV: You can send it to the traditional e-mail address, abuse@cctld.ru, and it works.

NIGEL ROBERTS: Thank you very much, indeed. Thank you, Andrei, and I hope you'll join me in thanking all of our presenters on this security topic. Byron?

BRYON HOLLAND: Again, thank you to all the panelists. There was much, much interesting information there, and even a few laughs. That always helps first thing in the morning. I'd also like to thank Nigel for chairing and being very good with his time management – so good, in fact, we will have a few

extra minutes for the coffee break, which we will commence now. Just a reminder that we will be back at 11:00 for the next session. Thanks.

[break]

UNIDENTIFIED MALE: Do we have [Tang] from CNNIC? Thank you for coming to one of the most popular session in ccNSO. We have a meeting. Yes. Good morning.

In this session, we have five presenters here. Kirsi from .fi, Andrew from Calzone, and Xiantang, Tang from .cn, and Crystal from .co, and Jay from .nz. So, the first presenter will be from Kirsi, from .fi.

KIRSI SUNILA-PUTILIN: Okay, hyvää päivää kaikille. That's "good morning to everybody" in Finnish. My name is Kirsi Sunila-Putilin, and I am legal counsel for .fi, and I am going to talk about our organization a little bit first.

So, .fi is actually part of this organization called "FICORA," which means Finnish Communication Regulatory Authority. And we don't do only the running of the .fi. There are also other things going on.

We have 250 people working, and if you look at some of the things that we are doing, is the spectrum management and also the security. There you have the national CERT and also, nowadays, actually, starting from the first of January, we also have the National Cyber Security Agency in this security area.

We used to have a domain name [unit] that was part of the security, but nowadays, we have been moved to stakeholders. I will tell you more about that, also.

But, anyway, markets. We are supervising the telecom markets. We have the economic supervision plus the technical supervision. This is the stakeholder's division, and there, the .fi names are in the products and services. The head of that is Johanna Juusela. I'm sure that many of you already know him.

Since a new organization came into place, we also have some numbering question in our division, plus short-term radio and TV licenses and handling of undeliverable postal items. All the customer service is in the Information division. So, basically, all the questions about domain names and all the other things that we are doing at FICORA will be answered by Information, if possible.

So, here is a new Information Society Code. There is a proposal at the moment that is handled by the government – sorry, the Parliament at the moment. The work started already almost three years ago. There was a plan to gather all the regulations for electronic communications only to one act, and this actually now includes eight acts and about 490 sections that have been consolidated to form this new code. And now there are less sections after this work.

This proposition was submitted to Parliament at the end of January. If everything goes the way that it's planned by the Ministry, this should come to force in 2015. But, for domain names, the changes would take

place 2016, because there are some big changes going on and we need to prepare for them. That's the reason for that.

And the laws included in this code are the Communications Market Act, and then the Privacy in Electronic Communications, also the Radio Act and Act on Television and Radio Operations, and auctioning certain radio frequencies, and also Provisions of Information Society Services, and also this very little law that we have had, the Prohibition of Certain Illicit Devices for Accessing Protected Services. And of course, Domain Name Act, and last but not the least, of course, in my opinion. But, actually, this has not been the center of attention when it comes to this new Information Society Code.

And there have been important objectives to ensure the functional communications markets and to eliminate overlapping and to clarify and update the content of the regulations. But that has been, of course, a very ambitious plan for the Ministry.

And when it comes to the Domain Name Act that we've had since 2003, it's a very precise act. So, the ministry wanted to have some kind of study about what should be done with the Finnish domain name law. And so, the consultants, they were doing a study and they made suggestions to do liberalization of the [person] Domain Name Act.

The changes suggested are, for example, no direct registrations for holders anymore. At the moment, it's possible to have a direct registration for .fi. But, this change now is here, proposed, so that we would not have the end customers calling us anymore. It has been a

little bit puzzling for the customers because they have not been really sure should they contact us, or maybe the registrar?

And then, another big thing that actually is something that I cannot even be sure if it's going to happen or not, the opening up of the .fi. At the moment, you must have, if you're a natural person, you have to have a domicile in Finland plus a Social Security number, and you have to be 15 years. If you are a company, you must be registered in the Trade Register of Finland. Of course, there is a chance to have a branch, also but still, these are the requirements at the moment.

So, is this going to go through or not? That is something that I have heard some rumors that the Parliament might not be wanting to open up the .fi, but we will see what's going to happen.

And then, also, another change would be that the e-mail address can be used in informing about the decisions and dispute resolution and e-mail address would be like a really legal [process] or address. And the thing is that at the moment, I did not tell you what this before that, we also have in-house dispute resolution. So, we actually handle cases when there are disputes over who owns the domain.

So, this should actually speed up our process, because since we are part of the government completely, we have all these administrative laws, and at the moment, when we usually use the e-mail anyways to ask questions from the holder if there is a dispute going on, if they don't answer to us, we have to send a letter, and this is because an appellate court – administrative court – told us that this is the due process to do. So you have to make sure.

So we've been sending letters. Usually, the ones that actually want to breach the law, they will not answer to our e-mails anyway. It only slows things when you have a problem with some domain name, and it's a clear case and you would like to delete it.

And we have some changes also in the wording, but that's not so important, I think.

And then another big change would be that, at the moment, the way housing for the purpose of redelivery is actually forbidden. In the future, it would not be.

Then, now we have a blacklist at the moment. We have a blacklist that consists of insulting expressions and insight into criminal activity stuff.

You know, these kinds of lists always raise a lot of questions, and I think that it's very good that we're going to get rid of this blacklist, since I don't think FICORA is the right authority to say what would be an insulting expression, for example. It's kind of funny, because the way life is going that maybe something that is already on our list is probably something that Lily Allen is talking about and singing about on the radio. I'm sure that you have heard this song. But anyway, that would be in our list at the moment.

So, we'd had also some complaints about this and cases going to the highest administrative court. The court has been agreeing with us, with our decisions, but still I feel that this is uncomfortable for us to do, so I think that this would be a very good change in the law.

And also then, the domain names that are used globally or as a country code, they would become available for registration. They are actually on our blacklist as well. For example, HK for Hong Kong. There is a company in Finland that would like to have that, because they have it as a brand, but they can't have it at the moment.

And then the thing that I'm sad to see going away from our law at the moment, we have this situation where a [natural] person's first and last name, they are protected at the moment. If the domain name is consisting these two elements, then actually you must have that name or you must have a trademark that includes that name or a trade name.

For example, we have had already twice the case where this famous Formula driver, Kimi Räikkönen – maybe somebody is following Formula? But he's been very famous. And so, all these famous names are always the ones that people think that, "Okay, I'm going to register that and sell it to Kimi Räikkönen, because he's got loads of money, living in Monaco, he can't even have that name because of the rules that we have at the moment." But still, interesting.

And then we also have this new section suggested for us to be able to resolve clear type of cases. We will have a possibility to delete a domain name for maximum of one year without hearing the holder of the domain name. But this actually require us that the rights holder will contact us first.

And then, this is actually really not on you, that we would have the right to forbid the registrar to provide services to customers for maximum

one year if they don't abide by the law or anything that we decide. We also have regulations that must be abide.

So, then, FICORA can act to ensure information security by necessary means without hearing the holder or user of the domain name. This is now one thing where we try to enhance the information security.

It's stated clearly in the law that we have a right to do some measures. Of course, the measures must be thought carefully, first. It's not like you can just do anything that you want. But, some reflection, of course, is needed when you use this power.

And then, the last slide is actually here about some new important requirements for registrars. First, that they are responsible for the information security of their operations. And also, that they have to inform FICORA of security incidents.

These both new requirements are actually not new for the telecompanies in Finland. Basically, the telecom companies already have these requirements, and we have made regulations where we specify, "What does this actually mean?" We do have this right to make these regulations, and they actually now become more specific and also wider when it comes to the information security.

We try to ensure that the quality of the services of the registrars would be good, and especially the information security part.

And at the moment we have this open working group that is actually working on the regulation that we are going to have. We have like 40 people, 40 organizations that are represented in that group, and they

have this possibly to be involved in drafting regulations. We also think that this group is important for us in order to be able to understand what's going on and what they are thinking about all of this, and also already starting to inform the new registrars of the future that these are the things that we actually require for them to do.

Of course, we have to supervise that, and there are a lot of questions that are still unanswered about how we are going to go forward with all of this. But still, that's why the group is very important for us. It's giving us also the feedback on what we are doing.

And, now, the informing of the changes is going to be a really big challenge, since now, at the moment, we have a really nice and neat domain name law. You can always just say that, "Look up, the law is here." But now, if we say that, "Look at the Information Society Code," you actually have to find everything from the five parts in the law. So, this is, of course, a challenge for us, too, on our web pages, for example, and in all the other ways that we can find out – to inform about the changes.

Basically, that was it. Thank you.

UNIDENTIFIED MALE: Thank you, Kirsi. So, questions? Comments? Yes. Yes please. Put the mic on.

STAFFAN JONSSON: Thank you. Staffan Jonsson, .se. Thank you, Kirsi. This is of course interesting, since we're enabling countries. It's always interesting to compare, especially within the Nordic countries.

I was thinking about two things, actually. The first one, you mentioned – or rather, in these changes of law, will there be a change in the need for registrars to have local presence within the country? Do you know about that?

KIRSI SUNILA-PUTILIN: The registrars' local presence is not required, at the moment. So, there's not going to be any change in that respect.

STAFFAN JONSSON: There will be no change? Okay.

KIRSI SUNILA-PUTILIN: Yeah, yeah. Actually, the registrars, some registrars were active about saying this would be a requirement of the local presence for the holder, would be against the directive of services.

STAFFAN JONSSON: European market and internal market? Yeah, okay.

KIRSI SUNILA-PUTILIN: Yeah. And so, you know, for example, one ministry, the Ministry of Commercial and Labor Ministry, they were really feeling very strongly

about this. And also, another nice detail might be that we had a change of a minister during this process. The first minister was against the opening up .fi, and now the new minister is not. But, okay, yeah. Some history.

STAFFAN JONSSON: Another question is regarding the responsibility of registrars. And you say that you will regulate registrars' operations and their responsibility. How far does this responsibility reach? Is it just operations in technical terms, or is it also content of the domain name, per se?

KIRSI SUNILA-PUTILIN: It would be mainly be about the quality of the services, so that actually, they do everything that the law says and all the regulations that we are making, they must be, they must fall into our powers by the law.

So, we can't just regulate anything, and basically, we want them to do the business as they like to do it. But, the information security part is here now, the new one, and I think the most interesting part.

So the quality of the services, so that the customers are actually getting the service. We don't want to hear about the complaints, so if we start to hear about the complaints, that's the time when we will start asking questions.

And also, now this information security question, this is something that is new and that would be one emphasis on the regulation.

STAFFAN JONSSON: Okay. Thank you.

KIRSI SUNILA-PUTILIN: You're welcome.

UNIDENTIFIED MALE: Thank you. Yes?

ABIBU RASHID: I'm Abibu Rashid from .tz. The presentation was very good, especially the aspect of registry, registrar model, which is the best way to go to give the registry more concentration on registry management.

But, for opening up registration, I was wondering for myself, what are your plans in terms of balancing of the checking? You said for the company, you need to check for the company registration. Now, once you open, and there is a foreign company which wants to register domain under .fi, what did the balance, in terms of checking up, since this is a foreign entity?

KIRSI SUNILA-PUTILIN: When we open up the .fi, that really means that we open it up. Since, at the moment, we don't even check, it's like an online system. If you want to register a .fi name, you can just do it and give us information.

But if there is a problem and we find out that you actually are in breach of the law at the moment, that you are not a company registered in the Finnish Trade Register, then if that's the case, then we would start

asking questions and saying that we will delay the domain because it's against the law at the moment.

But so, when we open up, if that goes through, it means, really, that we are not really checking anymore of that data, because if it's open, then it's open.

But, of course, what is not changing in the law is that if you give false information to FICORA, you will end up losing your domain name if you don't correct that data. We have that in the present law. If you are interested in the present law, we have the web pages at FICORA and you will find material in Swedish and in English. You can find the translation of the present domain name back as well.

UNIDENTIFIED MALE: Okay, thank you. So, for the interest of time, I want to move to the second presenter, who is Andrew from Calzone.

ANDREW BARRETT: Thank you. I am Andrew Barrett, I'm from Calzone. Calzone is a free productivity tool for trademark lawyers, business owners, and marketing managers, to help track, organize and prioritize all events and news related to TLDs.

We believe that there is a lot going on right now in ICANN. There is hundreds of new gTLDs coming out on a regular basis. There's already 270 ccTLDs out since the 1990s, and the marketplace is becoming increasingly competitive. And we ask the question, "How does one

stand out and ensure that their news, their policy changes, reach their target audience?"

We currently support all new gTLDs and their key milestones, such as from when they sign an agreement with ICANN, to reaching delegation, sunrise periods, throughout general availability, and so forth. We are designed to give these TLDs exposure and allow them to reach trademark lawyers, as I mentioned earlier.

Let me show you how it works. This is a live site. If you choose to follow along on your laptop, you can go to Calzone.org. We have actually aggregated all relevant information for TLDs. We have it organized by agreements signed, delegation, startup plans. You can sort and filter through all TLDs based off of industry categories and even internationalized domain names. For example, if you are a Russian script TLD, or a Chinese TLD.

I am here to invite you to submit your events to Calzone, because we believe that, with the increasingly competitive marketplace, something has to be done to help people gain exposure and reach the right people. As my colleague to the right of me said, .fi possibly is opening up their registration, a rumor. This would be great news to tell people. How do you tell people? Of course, the usual channels will be conducted. But Calzone is also a great supplement for these channels.

I have people coming up to me this week, telling me that Calzone is now their new homepage. These are trademark lawyers. They are always keeping track. They're checking the website every day for new events.

And the best part of this is, users can subscribe and add custom alerts to their calendar, their phone, whether it be Outlook, Facebook, Apple, or Google. So, let me show you how we can do that.

Earlier this month, .co.com entered a recent sunrise. Simply a click of two buttons, and you're allowed to set up a customized alert to remind you of all this information on whichever platform you utilize.

Now, I believe that this is important for ccTLDs, because there are many policy changes that are happening that are becoming lost amongst the masses. There's a lot of news happening, and a lot of people are focusing on gTLDs, but this is simply a distraction.

It would be highly beneficial to everyone to submit events and participate in this act of community and ensure that ccTLDs reach the eyes and reach the people that are distracted by the gTLDs.

Now, I'd be more than happy to take any question you have at this time.

UNIDENTIFIED MALE: Questions? Okay, thank you very much, Andrew.

ANDREW BARRETT: Thank you.

UNIDENTIFIED MALE: The third presenter will be from Tang, from CNNIC.

XIANTANG SUN: Okay, here we are. Thank you, Chair. And hello, everyone. My name is Xiantang from CNNIC, China. And today, the purpose I'm here is to introduce some experience on what happened in the past three years when the new gTLD thing came into the Chinese market.

So, and as CNNIC strategy, we really focus on the national market, the Chinese market. And then here, we want to share our experience on what happened in the past three years, and what we're going to do in the future, especially in this changing fast-changing world. There's going to be several thousand TLDs going into the market very soon, and the IG, Internet Governance, issues are becoming more and more popular, and NTIA gave the announcement on ICANN globalization. And we do need to redefine our role as the ccTLD manager in the Chinese market. So, this is going to be a little story for everyone to share. Next, please.

So here is some numbers to update what happened in the latest market situation. So, first of all, I will say, I'm quite happy with the numbers. Slow, but steady growing. Three years ago, .cn dropped to no more than four million, but today, we're going up to almost 10 million again, to occupy almost half of the market. Until last December, according to our statistics, we have .62 billion Internet users, and almost half billion mobile users, and some other numbers, you can see from the picture. And the real name of .cn is reaching 99%. So, that guaranteed the quality of the registrations, so we are quite happy with that, although it does reflect some facts of the economics.

So, according to my knowledge, I believe the reason for the number is going up is, first of all, is the government. They put a lot of money to improve the fundamental information resource. And, as a national

strategy, last months, the government gave the regulation policy, to say almost everyone, almost with no cost, could register a company that will improve .cn's number rapidly.

Also, there are the innovation things like cloud computing, things of the Internet, e-business, big data, mobile Internet, and also the cheap price of intelligent mobile that bring a lot of more and more Internet users in the Chinese market. So, we're quite happy to see the number growing very, very – not that fast, but slow and steady with good health.

And according to our opening, the market is huge. It's big. And the reason I'm here is to introduce the story and want to bring more collaboration. So, if any organization ask if they want to go into the Chinese market, please come to us. We, CNNIC, as a national platform, we really want to share the experience and also the market, want to be the hub and the bridge.

So, yes. Now I'm going to say a little bit what happened in the past three years, what the new gTLD challenge really come to the Chinese market. So, as the CN manager, we really got used to the .cn experience. And at the beginning, we really feel a little bit panic, yes, and feel at the situation is becoming more and more challenging, because it's going to be like hundreds of the new gTLD going to the market and compete with .cn in the market.

But, later, we found, this is an absolutely good opportunity for us to upgrade and improve our technology platform relationship, including with the government, with our partner. So, three years ago, we defined this strategy, we really 100% get ourselves into the new gTLD thing. So,

we defined from [inaudible] so we define our system. And we going to fully use our .cn channels, machines, servers, and registrars and all the market's channels in our 32 provinces.

So far, we improved, we define our new system, tailored from the .cn system. And also, we set up our research lab to research hardware to anti-DDoS attack equivalents. And we keep fast deploying resolution news all over the world, and then we improve our international relationship, especially to keep good relations with our neighbors.

So this is the system functions we designed, tailored for our new gTLD. Actually, we have already applied the IDN .com and .net, and we're also going to commercialize our platform providing service for other registry users who want to share the Chinese market.

Later, when we further get into the new gTLD market, we found that international collaboration is a key thing. The Internet is a one Internet that's global, so without international collaboration, we can't improve our technology and operation experience in the fast and most effective way. So, we're working very close with ICANN and CNNIC. We have the EBRO, now we one of the three EBRO operator. We have now already two or three real time exercise with the ICANN to test whether the service is stable.

And as the .cn, actually, we have three real time exercise, three times a year, and we have three data center deployed in the west of China, and then two in Beijing. So, anything happened, a bad thing happened, we can switch the service to other data center in, let's say, into ours.

Also, we just applied the Data Escrow Agent from ICANN, and now, at the moment, I think we are the only agent in Asia to provide data escrow service. The reason we apply it is to provide a tailored and more specific service for the Chinese users. And of course, we welcome our Asian neighbors to join us.

And also, for the TMCH certificate, we would really love the idea, because the Chinese market is quite big. We have huge amount of companies that don't know ICANN. They don't even know English. But, they do need TMCH to protect their rights. And we speak Chinese, and we use [inaudible] so we know the local market, thus the reason we really apply the TMCH certificate. And then, by using this agent, we are looking forward to working with our neighbors, working with ICANN, to make the protection of rights really happen. It's not only [inaudible] on the paper, especially for the local markets.

And last, but not least, regarding the international collaboration, we just applied a domain name [industry] training capacity building program in the APEC structure. So, fortunately, we got shortlisted, but we haven't got a final result, so I can't say more detail. If we're lucky enough, we will invite more neighbors and our colleagues here to join us to see how we going to build things together. And the APEC meeting this year is going to happen in Beijing, so we're here again as a member of the organization. We sincerely invite all the members to go to the APEC. If you go, please let me know.

Last, Internet Governance. Our philosophy to build our own Internet Governance Research Centre is to develop in a better way. So, development is a key philosophy, and the methodology of how we

understand the Internet Governance. Our purpose for the Internet Governance Research is to make better the development. And in the future, we want to use the Internet Governance Research as a small hub to link with the world, to link China with the world. We want get involved, and we're looking for more friendship and partnership.

In the future, we are really looking forward to make CNNIC and also our research center as a small hub for the new gTLD in the Chinese market. And we welcome everyone.

Also, we want to be the hub for ICANN support. We can help ICANN to support local community to enjoy more service, like EBERO, Data Escrow, TMCH, etc. And we want to a hub of sharing research results, sharing the market, technology, registrar channels, and the public relations with the regional neighbors, to go into the Chinese market because we have been here for more than 15 years. We want to be a national, regional hub of Internet Governance Research. So we want explore more opportunities, especially in this fast-changing world. So we are facing challenges, but we also see this as opportunities we want to share and want to work with our colleagues.

So, that's it. Thank you. Any questions or comments would be very welcomed.

UNIDENTIFIED MALE: Yes. Do I have any comments? Questions? No? Okay. Thank you.

XIANTANG SUN: Thank you.

UNIDENTIFIED MALE: Thank you, Tang. Next, will be Crystal, from .co. Yes, here we are. Crystal?

CRYSTAL PETERSON: Hi, everybody. My name is Crystal Peterson. I am the director of global sales and channel marketing with .co Internet. I'm very excited to be with you today to share a little bit about the exciting growth that we've seen with .co over the past three-and-a-half years since our global launch in 2010, and share a little bit about what we feel attributes to some of that success.

.co has been, and will be, a ccTLD of the country of Colombia. I was delegated by IANA 23 years ago, and was only available in the third level up until the global launch.

Over the course of about ten years, the country of Colombia debated the merits of opening up the extension and what would the policies be, and they decided to move forward with that and opened up registrations so that there were no restrictions, and also opened up the second level, which had never been opened before.

And what we see today is some phenomenal growth, from 28,000 registrations when we took over the registry in February of 2010 to just under 1.7 million today. I know the slide says 1.6, but I'm happy to announce that as of, probably the end of this week, we will hit 1.7 million registrations.

Over the course of the year as well, the Ministry of Colombia was debating the merits. They put out an RFP to look for companies that would be able to take the domain administration into the next era. So, in 2008, we formed a company to be able to submit the RFP. And we were very happy to win that RFP in 2009 against some very stiff competition with the likes of companies backed by Verisign, companies backed by Afilias. Our small little four-person company, with partnership with New Star, won that bid. In 2010, we launched the domain with some great fanfare and very exciting times. Until we get to today, where we have just under 1.7 million domains.

And today, we've taken that domain and we've built a brand around the fact that .co is short, memorable, very SEO friendly, and a global extension. And one of the things that I do want to highlight is today I'm talking mainly about our global brand. We do also build our local brand in Colombia, and a lot of the strategies that we use with our global brand building, we also take and use those same strategies to build our local brands. So we have two brands that we are building, but here today, I'm mainly talking about our global brand.

So, for us, it really is all about the brand. 25 years ago, 26 years ago, when the Internet was getting started, the innovation was the fact that the Internet was here. And over the course of that long history, we saw that domain names became rather de-commoditized. So it became about what you put on the domain name, it became about all of the great things you could do after you had a name, but those letters, to the right of the dot weren't as important, and you would just get a domain, because we did not see a lot of brand building with those extensions.

So we knew that when we were building our strategies to launch, that in order to be different, we needed to de-commoditize our product and be about the brand, because we knew that in the global market, we were competing against that 800-pound gorilla that has over 115 million domain names today. And how could we differentiate ourselves to build and take a piece of the pie in the domain name market?

You know, to us, it wasn't about being a gTLD or a ccTLD, or a domain extension, or any kind of acronym. It was really about bringing a brand to market, to create happy users that wanted to come back again and again, and renew their domains again and again, and find a place online for their dreams and their businesses to be able to be built.

We wanted our brand and our domain to be about the way people interacted with us, and not just about getting a website or a web address. So with that, we build a strategy around three pillars and a secret special sauce, we call it. We have awareness, growth, and use, with a secret special sauce of engagement.

Awareness, from brand building and mass awareness to consumers, which was something different that most domain extensions hadn't necessarily done before.

Growth, from building programs with our registrar channel, and placing the domains so that people could find it and be excited and see the brand when they went to their registrar partners to buy their websites.

To use, finding high profile use cases within our target market and within the larger brand marketplace, to really extend their brand

presence and not just protect their brand, so, you actually saw it out in the wild.

Some of the mass awareness cases that we did, we were excited to do three Super Bowl ads with GoDaddy. We've had billboards that we've seen in Times Square, things of that nature. But to really be different and do different things than a typical domain name. One of our favorite statements internally is the fact that we'll get e-mails from .co website owners that say, "I never really knew the company behind the domain. It's really weird for me for my domain name company to contact me, but I like it, and thank you." That's really exciting for us.

From the growth perspective, over the course of these past four years, we've done the majority of our marketing in the U.S., and so we have seen a big expansion in the U.S. Now, and going forward, we're also starting to look into additional markets and how we can grow even more exponentially those additional markets, looking definitely into Europe and the Asia regions. But, being able to really partner with our distribution channel, to be able to grow that placement.

And then from use cases, really being able to partner with tech companies, partner with big brand innovators, and help them extend their brand so it's not just about protecting and just getting a domain and forwarding it to your main domain, but how can you really use your .co to extend your brand presence online?

But for us, and one of the things that we love to talk about and everything that we do drives towards the moment of engagement. The domain purchase, for us, is the start of relationship. It's not the end of a

relationship. So, we want to be able to create enthusiasts that will then turn around and tell their friends about some of the great things that they've been doing, and be able to really engage with our customers, to have them come back again and again, which, on the technical side, creates more websites, which creates more renewals, which creates more revenue, which is all the fun stuff of the technical. But, really, what we want to do is we want to be able to see the smile on every .co owner's face about the fact that they have a .co and they were able to do something cool.

Some of the things that we've done with that, from engaging on Facebook, engaging via e-mail, engaging via Twitter, with a lot of our .co owners that we find in the wild through Google searches, through Yahoo searches, just through now being able to drive down the street and seeing a .co is fantastic, to also being able to engage them with different programs that we've been building that I'll be able to tell you about in just a few moments.

An example that I have that we're really excited about is a website owner at the website, deconstruction.co. They had applied to be with us at an event in New York City, called the Next Web. And they came and they were able to present in our booth for free, due to the plan that they submitted and the fact that they were on a .co. There, they were able to meet Werner Vogels, who is the CTO of Amazon. They were able to speak to him. He went on to do the presentations that he was doing during that week. And two weeks later, while he was on stage giving a keynote somewhere else, he mentioned deconstruction.co from that stage, which was live streamed and taped live.

So with deconstruction.co being able to go from applying to be at an event where they were never planning to be unless they had done through our booth, to being recognized by the CTO of Amazon on a keynote stage, to us that's just some of the ways that we can help engage with our audience to create that enthusiastic marketplace.

And one of the ways that we do now is through a new program that just launched in November 2013, last year. We call it the ".co Membership Program." With this, after the domain name sale, this takes that relationship one step further. This is a place where, outside of the web services activity, web services that people buy from their registrars, they can get event tickets, they can apply to be at events with us, they can get access to webinars, seminars, SEO tools, everything that they need to be successful and create successful websites. And beyond a successful website, create a successful business, blog, whatever it is that they're looking to do.

We're very excited about this program. We've seen an upsurge in traffic to the site. We've seen an upsurge in some of the excitement around the domain. At one of the events that we've been to over the past three years, with the implementation of the membership program, we went from three years ago, being able to contact and access three .co owners, to this year, being able to have access to over 188 people that have .co websites or are connected with .co websites, through a lot of the promotion around the membership programs. So we've seen some great results, and we're looking forward to seeing even more and how better we can engage.

And then, additionally, it's not only about engaging with our .co website owners or .co users – we dub them ".co-ers" – but for us, it's also about engaging with the other side of our channel, which is our registrars and resellers, who I am the main relationship manager there, to some of the partnerships that we've been able to build over the years. Always we want to be able to engage with our community, to create smiles, to create happy faces, which in turn, will create revenue, which in turn, makes them winners, and ultimately, then, the registry a winner too.

And from all of the vast awareness that we're creating to the growth that we're looking to build and to the use and the engagement that we want to see, we are really looking forward to 2014 and beyond, and how we can help to create .co as the brand of choice for starters, innovators, tech companies, and really be able to find our place within the large local brand market that's already here, and gTLDs, to all of the new TLDs that are coming into the marketplace now, and to still have .co remain relevant and still the fastest TLD in history. Thank you very much.

UNIDENTIFIED MALE: Thank you, Crystal. Do we have questions? Comments? Yes. You're the second.

LISE FUHR: I'm Lise Fuhr, I'm from .dk Thank you for a very interesting presentation. You talk a lot about .co as a brand. Do you have a strategy for the branding of Colombia?

CRYSTAL PETERSON: Yes, we do. Thank you for that question. The strategy that we've built, which I had mentioned earlier, around awareness, growth, use, towards engagement, it's the same strategy that we have now taken into our local market. Our local market has always been there. It's been there for 23 years, because of the fact that we launched 23 years ago with .com.co, and some of our other TLDs. But as we have been growing the global brand, we wanted to take that back and say, "How can we increase awareness and increase pride in the local extension to be the extension that Columbians choose when they want a Columbian presence or they want to be associated with Columbia?

So we use those same strategies. We've revamped our website in Columbia. We have a specific website for Columbia. We have been growing and building plans around creating some awareness and some advertising. We do programs with our local market and extending the distribution channel there for the local brands, as well as then being able to highlight some of the great use cases.

Use cases are slightly different in Columbia because most of the large businesses already have their .com.co, so when we get excited about finding one .co out in the wild somewhere else or finding five .cos, there were 28,000 when we already took over the registry, but now it's about finding the use cases that we can highlight from what we call the new area.

But yes, we both build our local brand and our global brand, and they're both very important to us.

UNIDENTIFIED MALE: Okay, thank you.

UNIDENTIFED MALE: [inaudible]. You've been mentioning that specifically to address registrars as well but haven't been too specific about it. Could you elaborate on it a bit?

CRYSTAL PETERSON: Let me make sure I understand your question. So just talking a little bit about some of the conversations and how we work with registrars? Is that it?

UNIDENTIFIED MALE: Yeah. From the presentation, what I saw is that you've specifically been addressing with certain programs like visits to VIP venues and stuff like that, what I take as invitation to registrants – so, private persons.

Following that, you've been mentioning that you do address you registrars specifically as well, so I was wondering what the specifics about addressing the registrar channel would be.

CRYSTAL PETERSON: Excellent. Thank you for clarifying. Taking a step back, we do have a registry-registrar model. All of our TLDs and all of our products, except for the highly-restricted domains are sold solely through registrars. We do not offer those domains through the registry at all.

With that model, there are branding and assets that we like to give to the registrars to help drive the message to the registrants in the way that we are building their brand. So from assets to copy to messaging, we are able to give that to our registrars, and the ultimately as well, as we've been growing over the past three-and-a-half years. We have different types of programs, from sales and promotions to particular influence in one market or another, and be able to talk with our registrars there about what are some of the things that we can do together to grow your business with .co, which of course ultimately will grow our business. So it's from assets, but also, as I mentioned, sales and promotions, too.

UNIDENTIFIED MALE: Thank you.

CRYSTAL PETERSON: You're welcome.

UNIDENTFIED MALE: Thank you. Next?

JOHN: Hello. I'm John from .id. Nice presentation. Thank you for sharing with us. It's really interesting seeing that .co is growing so fast here. I'm really interested to see what is the fundamental change in terms of the policy? We know that [inaudible] representing your country, and now you're already globalized. Thank you.

CRYSTAL PETERSON: Thank you for that question. The question was, "What was the fundamental change from Columbia to help open up the extension and make the way for the growth?" Yes?

When Colombia was putting the policies together and when they opened up 23 years ago, the TLD was a closed TLD, meaning you had to have a domicile in the country of Colombia. You had to be a business, and you had to have a business license.

From 1991 when it opened to 2010, it had grown to 28,000 registrations. The TLD was also extremely expensive. I believe at the time it was about $90 US to get a .com.co. When the TLD opened up, they domicile restrictions were taken away, just as Kirsi from .fi was sharing that they are considering as well. So there are no domicile restrictions on .co or .com.co. There are still some restrictions in ourwhat we call our restricted domains, which are for the government of Columbia.

Also, we lowered the price for .com.co. It went from about $90 US to you can find it in the marketplace anywhere from I'd say $9 or $10, and depending on the registrar, up to about $18 or $19, depending on their pricing model. So the barrier to entry to get a domain was lowered.

In the global marketplace, .co, which had never been opened before, the pricing was a little bit higher, as I'm sure you can see in the marketplace, but there are no domicile restrictions. So it's a very open TLD. IT has policies in place that are very similar, if not the same as

other gTLDs, so it made it very easy to implement by the registrars and able to get onto their platforms.

JOHN: In terms of your policy and domestic policy, do you have some constraint from your local community government [inaudible] that makes you going to global? What was your constraint? Admitting that everyone is your community except that you're going global, and especially change turn from a country code to be the [a brand]?

CRYSTAL PETERSON: We still consider ourselves a country code, and we still have a product for the country code. Our mandate from Columbia was to grow the extension and open up the extension, and so we worked with them and understood that to be that the new domain space, which was the second-level domain space, would be a global extension. That was with their blessing, and they knew that we were going to do that, but that is where we understood to grow.

But we still have our local extension, and we still are a ccTLD, and that is very important for us to also grow the Columbia name space that was already opened, but to grow that larger.

For instance, as I mentioned, in 2010, we took over the registry at 28,000 domain registrations in the third level. Now we've grown that to over 120,000 domain name registrations.

So yes, globally we have 1.7 million, but we have almost doubled each year in local registrations as well, which we're very proud of.

JOHN: So it means that you are feeling fine that some of your subdomains will be global, and some representing your country code?

CRYSTAL PETERSON: Yes.

JOHN: Thank you.

CRYSTAL PETERSON: You're welcome.

UNIDENTIFIED MALE: May I have the last question to Crystal?

UNIDENTIFIED FEMALE: Hi. [inaudible] from .om ccTLD. I believe that .co has a similar situation to .om. We have a similarity like the .com. I believe that we have the same similarity with the .com and .co and the .om. We have one letter. When you drop one letter, it's a similar TLD. We have been reached by several companies. They want to implement their wild card, and we have been under pressure to implement the wild cards. I want to know .co's stance on wild card service.

CRYSTAL PETERSON: That's an excellent question. We actually don't allow wild card services. That was something that we put in place when we launched and was a policy we put in place because part of our marketing guidelines is the fact that we did not want .co to be marketed as a typo, or as a place to be able to cybersquat on domains and have a worse reputation for that type of activity. So we don't allow wild carding at all as we launched.

UNIDENTIFIED FEMALE: Thank you.

CRYSTAL PETERSON: You're welcome.

UNIDENTIFIED MALE: Thank you. Thank you for running an interesting presentation. The last presenter will be Jay from .nz.

JAY DALEY: Good afternoon, comrades. It's nice to address you again. So a brief talk about marketing in .nz. I'm Jay Daley from the .nz registry. The slides are weird. Let's do that again. Okay. That's how that works.

Why did we begin marketing? This is an old chart. It shows our growth versus our budget from January 2006 to December 2008. You can see the net growth per month. You can see our budget, which was generally set in October, following where our growth had got to – our rolling twelve-month growth. And you can see it all going very horribly wrong

in 2008 – a little thing called the global financial crisis, I think. That I'm sure was common to many people, but in November 2008, we had something quite unprecedented. We didn't grow in domain names. We reduced in domain names. We had to rewrite some systems to cope with that on our marketing side of things, on our data analysis side.

So we set out some goals for marketing. The first one was long-term financial stability, which comes from three elements: more sales, growing the marketing, more sales by people switching from gTLDs. We currently have about 68% of the market of domain names in New Zealand. And then from a higher renewal rate, which I know other TLDs have been very successful at doing.

And then the next goal was in enhanced recognition. We found that we are, like many codes I suspect, have a good reputation, but no recognized brand. People in many cases don't even know that there is a company that runs the TLD.

So after seven years of negotiation, we recruited a chief marketing officer, David Morrison, and this presentation is all about his work. He gets all the credit, and if anything goes wrong, speak to him as well. Hi, David.

Okay, just the outline plan then, and I'll talk through all of these very briefly. We set out trying to get some evidence. We need to know exactly where we're going from the evidence, so that was market research, which we then analyzed. Then the development of the brand, the three parts: the territory, the positioning, and the brand expression. And then the marketing: the marketing strategy, who we were

targeting, what assets we're providing, and how we would then use those in campaigns.

Part One: The Evidence. We contracted with a leading market research company in New Zealand and ran two surveys, one for a consumer survey and one for a business survey, reaching 1000 people each time. From that, we were able to understand really why people like .nz and why people use those names. We have those reports from each of those surveys publically available for you to access on a website I'll show you later.

We also then looked at ex-registrants taught with cooperation from registrars to send them a brief survey when they were cancelling to find out why they were cancelling as well.

From our main survey then, we wanted to understand how people find products and services. 97% of people looked for products and services using an Internet search. Next I think is about 60%, but it's cut off here, was word of mouth, and then television, and then the other types of way.

So Internet search now entirely dominates the way that people go and find a product or service. If you need an electrician to come to your house, people use Internet search much, much more than any other channel.

This then leads us to a gap. We have 97% of people searching on the Internet for products or services, but only 34% of businesses with a website. So there are 66% of businesses out there that are largely inaccessible to the people who are searching.

Then we looked at who do you trust in the brand namespace and why. This is a very, very clear answer, really. .nz – high level of trust. Extremely high level of trust, and trusted because it is local. There isn't much more to it. It's not necessarily about it being secure or being low-priced or anything like that particularly. It is about it being local. This is a very strong cultural affiliation.

Then we needed to understand how people use .nz without going to .nz websites first. Do people filter searches for .nz? These are some great numbers, and I think this might be replicated in many of your countries. 89% of people specifically look for .nz domain names all the time or sometimes in searching through the Internet because of this trust thing, because they're local. And 78% filter their searches with 79% typing ".nz" or "nz" as part of the search all the time to ensure they get that.

The main search engines have specific sites for New Zealand. There is a Google.co.nz, but even with that, people still personalize their search further by adding in their country code.

So that was our evidence. Then from that, we're able to start developing the brand. The first bit is the territory and positioning. We keep that confidential, but it's very much business focused. We have a three-level domain name structure currently, and so people are able to register in .co.nz or in .org.nz, and a very high percentage of domain names are in .co.nz, so it's very clear that it is primarily businesses that register domain names within .nz. Looking at that and the gap identified previously, that's very much the territory that we need to be in.

Then there is the brand expression – the logos – and this is a revision of the established expression that we had. Not a huge change – here it is, the .nz bit. I'm probably going to get complaints from Norway. We've stolen their black but we had it first, I'm sure.

The strapline can change as needed, but it's very much helping people understand that this is the beginning of a journey and moving forward in terms of their online presence because we can't complain that a domain names does everything for you. You need the domain name, then you need the website, then you need the search engine optimization, and then you need the other things. This is the start of a process. A very important start, though – in fact, the most important start, I think.

Then onto the marketing. This is our marketing strategy. Effectively, we need to achieve three levels of things. The first is the awareness: people actually understanding that .nz is not just a thing that just sits in the background; it is a conscious choice that you should make and why you make that conscious choice and what form of organization that is that you are then consciously choosing to transact to it.

Then moving to the conversation so that people are then developing that awareness, and then into the transaction where informed people then by .nz domain names because they know that buying the .nz domain is the best way to reach the local market or because they want to particularly base it on those attributes of trust and localness and other things.

So these are our targets and it's kind of weird. We have 80 registrars. We have maybe 1000 active resellers. Our reseller chain is probably 20,000-50,000 big, but 1000 of them are active. 50,000 influences – our view of that is, when people buy domain names, they regularly talk to someone to ask them, "Please give me some advice." That could be the IT technician in the organization. That could be the accountant, some small business advisor, and these people are actually very important because, while each one of them may only influence one or two transactions per year, that's a very big portion of our registrar.

Then there are 470,000 businesses within New Zealand, of which about 450,000 are small businesses as well – small to medium enterprises. Then we have a population of 4.4 million people.

If you look at things like mobile phone usage or cars, there are many countries that have far more mobile phones than they have cars, so I think it's entirely – sorry, more mobile phones than they have people. So I think it is entirely reasonable to aspire to everybody having two domain names in a country so that we can go to a nine million registrar in time. Okay? I hope.

Right. So then our assets. We have an informational website, "Get Yourself Online." On that, we have guides. We have research, and we have plenty of videos.

We need to be careful about informational websites in this way because we don't advertise to people and say, "Come to us." We want to advertise to people and say, "Buy domain name from a registrar." But there are some of those people who want more information and want

to learn more, and we need to provide somewhere for those people to arrive to help influence that.

We also need somewhere whereby those influencers I talked about earlier can find the information they need that helps them explain to somebody why they are making a particular recommendation.

At this point, I'd like to show you a video. Eric, is that possible? Thank you. Right, with added sound effects. That's my fault for leaving it quite late to ask if that could be included. But the link is there. I'll be testing you all later to make sure you've watched right through to the end. Okay? Good.

Right, so then with the assets in place, we have campaigns – once we have all of these components in place, to start trying to change people's behavior. Much of that is around advertising, and all we've conducted so far are small-scale tests to make sure that we understand what are the best channels to work and how do those things work.

We've done a lot of work on business sections of news websites. Now, this actually works to our advantage, given that we are wholesalers, effectively. If you buy pay for click advertising in this way, you'll generally find that you can get millions of impressions, thousands of clicks, and you are charged for the number of clicks that you get through, and you are trying to get people to visit a website.

We are not at that stage. We are much more about awareness. We want people to understand that we are a brand and understand the attributes there. So for a relatively low cost, we're able to get millions of

impressions out there where people can see an advert without then following it through at all, and that works very well for us.

We've also used radio advertising, which has been quite good, and some social networking advertising. Finally, we've been able to use sponsorship.

So that's a brief run through then of things. You can contact me. Or better still, you can contact David, particularly if you have any complaints about the video. Let him know. Any questions?

UNIDENTIFIED FEMALE: It's possible that I missed it, but how many domain names do you have at the moment?

JAY DALEY: 550,000, approximately.

UNIDENTIFIED MALE: Questions? Yes?

PIERRE DANDIJNOU: Pierre from AfNIC.fr. Thank you, Jay. That was very interesting. You talked about the campaigns that you launched. Are you able to link the campaign with the increase of the registrations, for instance? Because every time we are spending money on marketing and advertising, we are not all the time very sure of the concrete return of it. I'm always asking this question to everyone who is doing campaigns.

JAY DALEY: Okay, it depends on what the campaigns are intended to target. Our initial campaigns are about targeting awareness of us as a brand, and so that is what we are measuring. It is the research that we showed earlier about doing those things there.

For us to target growth directly in registrations, we need to ensure that our advertising can bring people to transacting as quickly as possible. Now, currently with our advertising, if people wish to transact, they can go and do a search to find out about finding a .nz domain name, but if they know nothing about it, it's a tricky process.

We can bring them to our website, and from our website they can get a random list of registrars and move onto transact that way, but that's a very slow and cumbersome way of doing it, okay?

So for us to have advertising that is deliberately designed at making people transact, which we will do when we get to that stage, we need a different mechanism to do that, and we have yet to implement that mechanism because we're still trying to build the awareness of us so that people recognize that .n exists, why they have .nz, and how that compares to other TLDs that are entering the market.

JOEL CHORNIK: Hi Jay. Joel with .ph. Interesting thought: everywhere I go in New Zealand, all the billboards, all the papers, the use of .nz – not .com, but .nz. So I'm wondering why you think there's a need to build the brand? Everyone knows about .nz.

JAY DALEY: Well, we've done the research. People know instinctively some things about .nz but they don't know them explicitly, okay? They don't know that there is a company behind .nz. All this conversation where you say you work for .nz and people go, "Oh, was that a government department?" and that sort of thing. Or, "Is that something that happens? I didn't realize there was an organization there." Or if you start the conversation about, "Why do you like .nz?" the answer is, "Well, I hadn't really thought about it, but I suppose it is because," and then they all say the same thing: "Because it's local and I trust it."

We don't want that to be a subliminal conversation on the side of people's heads. We want that to be explicit. We want people to know that they have to follow that thought through and know that .nz brings those attributes to them so that they are much more consciously choosing .nz so that when they then see other TLDs with other attributes, they're able to then judge at a better level than just the straight instinctive level.

Finally, just to say that we get reasonably good stats that tell us that we have 68% of the market, and that can go up or down by 4% in a year as other TLDs run special offers or promotions or other things.

So it's not by any means a certain market, and going back to my very first slide as you saw, there can be occasional catastrophic impacts on our registration volume. So financial stability is the goal here, very much.

JOEL CHORNIK: Okay, thanks.

UNIDENTIFIED MALE: Any other questions? Okay, if not, thank you for the interesting presentation and interactions. Now let's wrap up this ccTLD [new] session. Thank you very much.

KEITH DAVIDSON: So everybody, we'll get this rolling in just a moment or two, but if the TLD organizations' representatives could come and join me on the stage, please. Can I ask everybody to take their seats? We'll get this session organized. Thank you, everybody. If we could take our seats and come back to order and maybe someone at the back could close the doors. Thank you so much.

This is the regional organizations updates, and we have four presentations and we have 23 minutes, so that's about six minutes each. So firstly, over to Abibu for AfTLD. The floor is yours.

ABIBU NTAHIGIYE: Thank you, Keith. My name is Abibu Ntahigiye from .tz registry. I'm presenting on behalf of Barrack Onteiro, who is the administrative manager of AfTLD.

I will give a briefing on what is happening in Africa on behalf of AfTLD. Basically there are three issues coming very soon. The first one is in terms of capacity building. We do expect it to have advanced registry operators [inaudible]. This will be alongside Africa Internet Summit from

26th of May to 30th of May. This Africa Internet Summit basically incorporates [ISTAR]. This is AFnoc, AfriNIC, and AfTLD.

Also, we have one other project: to build an observatory for ccTLD in terms of capacity building for DNSSNEC and hopefully this will commence in April or early May. AfTLD is collaborating with ICANN, ISOC, AFNIC, CENTR, and LACTLD.

The other activity during the 2014 is about Africa Domain Name System Forum, which will be held on the 7th to the 9th in Abuja, Nigeria. This will the second forum. The first one was alongside ICANN 47 in Durban, South Africa.

In terms of the board and the staff of AfTLD, we have the Chairman, Palos from .mu; myself from .tz; Erik Akumiah from .gh (that is Ghana); and Mario [inaudible] from .mg. That's in Nigeria. We have one assisting staff, Barrack Otieno, who could not make it here. That's it. Thank you.

KEITH DAVIDSON: Any questions? If not, can we move to Don and APTLD?

DON HOLLANDER: Thanks very much. I'll just go ahead and start while the pictures will arrive in due course.

I'm very excited about what's happening within the APTLD community. When I talked to you last in Buenos Aires, I had been here maybe a week into the role, so I didn't know much with what's going on. But now we have some exciting things happening.

During 2014, our focus in on information, education, and advocacy for our members. We've got a number of reports that we're planning for 2014. The first is on anycasting. The second is – oh, and we can show pictures. So the first one is on anycasting. That should be out in the next couple of days. The second one is on models for introducing new service.

Registrar accreditation criteria. One of the issues that came up in our meeting in Malaysia is how can registries and registrars in the region work better together? So we said we'd have a look at the different accreditation criteria that people use. We've done a survey of all our members, and we're also working with ccs outside of the region so we get a good spectrum.

We'll have a special report later in the year on registry solutions, so if you're looking for a new registry, backend or frontend, then this will give you some idea of things to look for. We'll also do a DNS Best Practice report, which is an update on the report that we produced in 2007.

The topics that we're focusing on this year are DNSSEC deployment. DNSSEC works technically. It just doesn't work for anybody's real benefit yet, so there's a whole range of things that need to be done, and we're working to identify them and identify the actors who need to deal with the things and put those things in place to actually function.

We've got a focus on engagement with the justice sector – ccTLDs and different models of how to engage with your police and law enforcement, lawyers, judges, and regulators. Security is a big topic for

the community, both for the registry and registrants, so manual locking and validation of DNS change requests. There's a number of models happening there.

IDNs is a constant topic for us. IDNTLDs do work. They resolve. They just don't work in real life, so it's the same sorts of issues around DNSSEC, and we have a good session planned for Oman if anybody's interested in IDNs.

Market developments, we'll look at that. Registrar-registry relationships, that will be a topic out of the Oman meeting. Internet coordination, which is Internet governance, only more focused. And we're looking at training opportunities for ccTLD managers, possibly towards developing an actual degree program.

This is our meeting schedule. We had a meeting last month in Malaysia. We had about 100 people there, which we were actually very pleased with. We have a meeting in Oman May 11th to 14th. APTLD's meetings are very open and very welcoming, so people in North Africa, for example, where the IDNs are also in issue, and in Europe, are more than welcome to come.

We'll have a meeting in the Pacific in September in Brisbane, and we've got a workshop in India in August as part of the regional IGF there, and we're going to talk about DNSSEC deployment, and we're going to talk about how to work with your law enforcement.

We had an election last February. There's our board. And that's it. Thank you very much.

KEITH DAVIDSON: Thank you, Don, and thank you also for sticking to time or ahead of time. Any questions for Don? Last chance. Okay. It's over to Peter and CENTR. The floor is yours.

PETER VAN ROSTE: Thank you, Keith. Good morning, everyone. As always, the CENTR update, or I think all the regional organizations updates, are obviously more pointers to what we do so that you can know who to address when you need further information on anything that we present on that we would have time to go into any level of depth during our six-minute update.

With that, first, looking at the current projects and from some follow-up from what I've told you last time. As I announced last time, CENTR started to look into the issue of registrar authentication and identification. The idea is: is there a need for a common platform, a common process, common description of tools? We're obviously not talking about the same authentication tool for registrars to authenticate themselves with every single ccTLD in that group, but at least is there a common basis? That's what we're looking into.

We had a working group on this. The initial results were there is still a lot of work before we can even agree on a common tool. That group is going to launch a survey. That survey is going to registrars. I'm also going to send it out to other ccTLDs outside of Europe who would be interested in that project. Let me know if you want to participate.

Secondly, we have a Security Working Group that is working on a security incidents repository. The decision at the moment is to go for a very basic form of repository, where confidential information would not be stored centrally, but at least pointers to security incidents and to relevant context, that would be included in there.

Then the third topic on our mind is obviously Internet governance. [inaudible] very well-synchronized with the other regional organizations. We are working on a position to outline our thoughts on the future of IANA in the broader context of the changing Internet governance models.

We've also drafted a paper on ITU together with CERA. That paper will be published I think next week. It's now in final draft form. The idea is to provide people with basic information before we go into a series of ITU meetings in the rest of the year.

And then the third thing is we're working together with the regional organizations on organizing another workshop during IGF this year in Turkey.

A quick reminder that the other region organizations, we have a stats survey. We have it every year. Last year we had 39 participants. The public report will be out pretty soon, but I'm ready to give you some teasers. I think this is one that tells a lot of stories. One picture tells a lot of stories. It's a medium domain name price for one year. What we see is that there is a significant difference between smaller and larger registries. The difference ranges from close to 12 euros that is exclusive

VAT for registries that are smaller than 500,000 names. Registries over two million names, their price drops to 3.4 – again, exclusive of VAT.

Probably the stat that every single one of you has already looked at in different shapes or forms, but they come out to the same thing, is the growth rate is decreasing significantly. If in 2009 on average – well sorry. The medium growth was still 15.3. At the end of 2013, we were just under 6% (5.9).

CENTR has developed a study together with Matthew Zook that goes and looks into the details of why we see that decrease summarized on a very high level. We found three elements that play a role. A very important one is the changes in the Google search algorithms, which probably will have had an effect on the number of part domains.

Secondly is obviously the pending introduction of new gTLDs, which might have postponed investments, in particular in domain portfolios. There are microeconomic trends, and obviously for some of the registries that have already a very high number of domains per capita, I think like SIDN. Market saturation might have played a role as well.

This is just to alert you to the fact that we have the study on the factors influencing domain name growth, that our statistics report is coming out, and that today we have also our monthly domain [wire] stats coming out. I've asked my colleague to send that to the list.

Future meetings it says, but there is actually one that I would really recommend. The others are available on our website. There is a jamboree. A jamboree is a meeting of all the CENTR working groups. Currently there are six working groups meeting during three days. The

idea is that we have synergies between the groups, that the legals start talking to the tech people and they come up with common IDs, for instance, on EID. The RND and the marketing groups are meeting, etc.

It's typically a CENTR members only meeting, but if people are interested, let me know and I'll get you in touch with the chairs of the relevant working groups. We'd be very happy to host you there. Thank you.

KEITH DAVIDSON: Thank you, Peter. Any questions for Peter? No? Okay.

Our final regional update is from LACTLD, and welcome, Victor. The floor is yours.

VICTOR ABBOUD: Hello, my name is Victor Abboud. I'm from .ec, and I'm here as a member of the board of LACTLD. I will do the presentation on behalf of Carolina, who is the general manager of LACTLD. I will start? Okay. Next slide, please.

In February in Antigua, Guatemala, we had a marketing workshop. It was different than what we used to do because we had registrars invited – something that in the past that was not done. It was good because we had presentations from them, and also we had a panel to see what were their expectations from ccTLDs in Latin America. It was very helpful. We had a lot of teamwork dynamics and good participation from all the members and it was in the end a productive workshop.

Also, in January, there was an SSR retreat in Montevideo. This is part of the security agenda of Latin American strategy that is being done among all participants. We had people from LACTLD, ICANN, ISSOC, LACNIC, and it was a fine day with a full agenda for the whole year of 2014 of different security meetings that are going to be in different months in different places.

As current issues, we've been talking too much about Internet governance, especially all the topics around NETMundial, some coordination with the other ISTAR organizations, and especially coordinating with sister regional ccTLD organizations.

Also, in May we will have a policy workshop in Cancun and also we will have the general assembly. In the workshop, we will focus, as you can imagine, on the IANA transition – whatever is new about the IANA transition. We will have a discussion on of ccTLD best practices, and we will have sessions regarding Internet governance.

As future projects and some issues going, we did this, but it's going on about Internet governance and so many new – we tried for the first time a webinar. It was a very good experience, and we will adopt that way of communicating with members. It's very useful both in Spanish and in English because we also have English speakers.

LACTLD is part of the Latin American IGF – the Latin American group for the IGF – and we area also coordinating with the other organizations the regional meeting for this year.

In terms of infrastructure projects, we are starting to work on a regional anycast network that would benefit all the ccTLD members of the region.

That's an update of more or less what's been going on from Buenos Aires up to now and what is going to happen until the London meeting. I don't know if you have any questions.

KETIH DAVIDSON: Thanks, Victor. Any questions for Victor? I thought there for a moment we were going to get a question.

Can I then take the chair's prerogative and ask a question of the regional TD organizations about ISTAR and your recent admission of all of you to the ISTAR community? How do you see that role developing given the other ISTAR folks are kind of in there to make decisions and be assertive? Do you see your role as being part of that group, or do you see it as a liaison back to your community, or do you see the ccTLDs that you represent could be bound by your decisions? Just any views on that sort of broad topic would be appreciated from any of you.

PETER VAN ROSTE: I'm happy to take that one. I almost heard a suggestion in that question. In September last year, the ISTAR group came out with the Montevideo statement, and within the CENTR community, there were questions on how our part of the industry was reflected in that group, whether we had any access to some of the statements that they made, particular the planning process that led up to those statements. At the time, there

was not, so together with the regional organizations, we sent the letter to ISOC – ISOC being the host of the ISTAR group – and they responded positively to our request to join them.

First meeting after that was in Santa Monica, and one of the general managers of the regional organizations was able to attend that meeting. It was Carolina. There she participated mainly to figure out what the ccTLD's role could be in such a gathering, and she participated in some of the wording of the statements that followed in the aftermath of that meeting.

What I personally think of the regional organizations' role is obviously to represent the ccTLDs' interests, not the ccTLDs. We have a pretty good idea of what our members want, and we are continuing the process to harvest that information through surveys and discussions. We also do, for instance, during the ccNSO meetings, I guess that this afternoon session will be quite revealing in that sense.

So we represent the ccTLDs' interest. We are obviously not making any binding commitments on their behalf – nor on our own behalf, by the way.

KEITH DAVIDSON: Okay, thanks. Is there any dissenting view from any of you? It seems to be a fairly full response. Okay, thank you. That's a very useful clarification. Thank you, Peter.

That brings us with one minute to go to the close of this session, so can you join me in thanking the four regional TLDs for providing their interesting reports?

I have one item of a general nature. Gabby and Christina have sent out the meeting survey form to the list and it's a reminder for everyone to participate. It's only through you telling us what you like and don't like that we can refine future meetings. So please do let us know what you're thinking.

And as the chair of this session, it's my sad news to be the first chair to tell you that we don't have a sponsored lunch today. We reconvene in this room at 2:00 p.m. It's the Internet governance discussion on the IANA database. The last 30 minutes of it, Fadi will be in the room to answer some questions and make some observations, so this is really, really one of the most critical sessions for us to start to focus on IANA. So please be back and we'll see you all at 2:00. Thank you.

[break]

KEITH DAVIDSON: Can I just ask people to try and move up forward in the room? We've got a fairly tight presentation that you won't be able to read, and it probably is quite pertinent to you. So please, move forward in the room. We've got great vacant spaces in the front and everyone tending to be at the back. Don't be shy.

Good afternoon, everybody. Again, I'll repeat myself. Please come forward. There's plenty of vacant space up here. We will be looking at

words on screen, so I'm pretty sure you can't read it from the back. Please move forward.

Hi, my name is Keith Davidson. I'm chairing this session as our fourth Internet Governance session here in Singapore. It's a community discussion defining principles and requirements for the IANA Function Transition Process from a ccTLD perspective. That's our challenge. We have 90 minutes to attend to this simple task. The moderator for this session, and the person doing most of the talking as we get through will be Byron Holland.

But we have two presentations to start. We'll firstly have one from Becky on defining "The What." Then we'll have a presentation from Jay, which is illustrating some models that might be the future. Then Byron will walk through Principles and Process. So, we'll have no more than 30 for the first two speakers, 30 minutes on Principles and Process, and then Fadi is going to join us in the room for the last 30 minutes, in which we want to pose the questions that arise along the way from this session to him. Do you have something to add, Byron?

BYRON HOLLAND: Yes, I do. Welcome to this session. Hopefully it's going to be an interactive session. We know that this issue significantly impacts us all, and getting your feedback and input through this is going to be absolutely critical. If I could just say, one of the things that I've noticed through the week is the changing landscape of this discussion. In a sense, what is the problem statement exactly? Not generally or overall, but exactly what is the problem statement that we're trying to solve?

Exactly, what does NTIA do that matters to us, that gap that is going to need to be filled?

The other piece is the process piece. How are we going to feed into working towards that solution with the broader community?

Yesterday a few of us took a stab at what the problem statement might look like, to put it out as a straw-man for us, as a community, to talk about. To say "Is this really the role that NTIA plays right now? Is there anything else we're missing? Can we come to some sort of general consensus on it that will allow us to start having dialogue about a process to inputting into the ICANN consultation, if we want to use that word for right now?"

So with that, we've put it on the screen here. Becky is going to walk us through it. We are actually going to take the time to look at it in some detail, because this whole issue is, to a great degree, an issue of nuance and words. And they're very important. With that, I'm going to hand it over to Becky.

BECKY BURR: Thanks. As Byron said, we're going to talk about two things. First of all, we're just going to step through what it was that NTIA said when it announced its intention to transition, and the INF functions. Then, we're going to look at just a straw man for what that means. What role the U.S. government is playing right now that we need to replace in this process.

So, the first thing is what NTIA announced is that it planned to transition key internet domain name functions to the global multi-stakeholder community. It called on ICANN to convene global stakeholders to develop a proposal to transition the current role played by NTIA in the coordination of the Internet's domain name system. So, NTIA is thinking that it's transitioning a role, and ICANN is being called upon to convene stakeholders to figure out how to do that. There's no presumption in NTIA's statement about what the outcome would be, what the end result of the transition would be.

NTIA, as Larry told us yesterday, set essentially four conditions, and only four conditions, which would be that whatever we all come up with it:

- Has to support and enhance the multi-stakeholder model;
- Has to be consistent with maintaining the security, stability, and resiliency of the Internet DNS;
- Has to meet the needs and expectations of global customers and partners of IANA services (and that's, as we talked about yesterday, very important to us because with respect to the domain name services, CCs are very important consumers);
- Must maintain the openness of the Internet.

Another point that's not in here, anything that the Internet global community develops consensus over is fine, so long as it's not a multi-national institution.

NTIA, in the announcement, described its role in DNS coordination, which is what it's thinking of transitioning as, and this is just with

respect to names, administering changes to the authoritative root zone file, and serving as the historic steward of the DNS.

So, the question that's become pretty clear this week is we all know what administering changes to the authoritative root zone file means, in a sense, but what we don't know, or what's not entirely obvious, is serving as this historic steward of the DNS.

So a group of us got together yesterday and tried to articulate what we thought of. We know there are things missing, and so one of the things that we need your help with today is figuring out what is missing from our list. But [Allen's] already mentioned one that I think is missing.

So, we know that the NTIA authorizes changes to the authoritative root zone. We know that it oversees ICANN's performance of those functions in the IANA contract. We know that it oversees VeriSign's performance of the functions set out in the cooperative agreement, and that's essentially taking changes that have been approved by NTIA and entering them into the authoritative zone. We know – and I think we forgot about this for a little while, we were talking about it – we know that actually NTIA both establishes the requirements and specifications under which both the IANA functions and the root zone management function are done.

So, when NTIA was drafting the newest IANA contract, it put the draft contact out for comment, and that was the way the community had input into the requirements. So it included things like – not just specific "Enter this," "Do that," – but it included things like what sort of automation should there be? What sort of consultation should there

be? What kind of documentation would be required? What are the SLAs? That's something that NTIA has been doing, but it's obviously something that somebody needs to do. We've had input into it, but it's clearly something that's transitioning.

As Allan pointed out to me, of course, NTIA actually chooses who performs the IANA functions under that contract, and who performs the root zone management functions. Then, NTIA also oversee ICANN's obligations to develop and implement consensus policies through a bottom-up multi-stakeholder process, as expressed in, but not limited to, the Affirmation of Commitments, and to be accountable to all stakeholders for the outcome of its decision making.

So, what we want to do here – and this is not going to be a one-time shot, we're going to iterate over this – is get input. Is this the right list? Have we missed something? Does something that we've got up here not belong? As I said, we know that there's one thing that needs to be added, and that's selecting the IANA functions contractor, and selecting the root zone manager.

BYRON HOLLAND: Thank you very much, Becky. I think you're good to go, but just before you do, like we started out saying, this was a straw-dog that a few of us thought "How do we isolate and start thinking about this problem in pieces that are digestible?" as opposed to a big amorphous discussion that, to some degree, has been happening throughout the course of this week. Our goal is to see if we can come to some common conclusion on what exactly the roles are, and have consensus on that, because that's

going to help us start to think about the process and then the substance of matters beyond the process.

That's how we got to where we are today. Of course, we had a very defined session for this one before NTIA made their announcement, so what we're trying to do here is as much as possible solicit input and feedback. We are going to have a scribe right here so we're not going to lose anything. I know we have a transcript, but we're also going to have a scribe take a picture of it and then try to, in very short order. work something back into this document.

Stefan?

STAFFAN JONSSON: Staffan Johnsson, .se. Just to be sure, are we absolutely sure about that the [IANA] functions will actually stay within ICANN?

BEKCY BURR: Well, we said that NTIA right now makes the selection for who the IANA functions contractor is, so that's a role that we have to transition. This does not predispose who that is, but the selection is an important piece of that.

KEITH DAVIDSON: Can I just introduce a slightly different thread, too? There are not many people in the room who are on Adobe Connect, but there are a couple of people who are not here, so perhaps if you join the room and

stimulate debate so people can absorb some more information, that might be useful as well. Thank you.

BECKY BURR: And you might also be able to see the text.

BYRON HOLLAND: That's true. And the other thing is feel free to use the chat if you want, instead of coming to the mike, either way, but we would like to solicit as much feedback to help us all with the thinking about this issue.

PIERRE DANDJINOU: Thank you. Pierre from AFNIC, .fr. It's more a question, but in the IANA texts they talk about IANA functions, with an "s." So, I'm not totally sure that NTIA is not speaking of also protocol parameters, IP addresses. I mean, I know yesterday the panelists told us, "No, no, no, we are not concerned." But I'm not sure.

BECKY BURR: So, the current contract does include a statement of work that has a variety of different functions, and it does include the parameter protocols in all of that. But I think, in truth, NTIA doesn't have much of a role with respect to that, but it is part of the IANA functions.

KEITH DAVIDSON: I think I understand your question and yes, that's transitioning as well. What we are concerned about is what the ccTLD aspect of the IANA

function will transition to, and being conscious that the protocol parameters, the IP address space, and the gTLDs will be transitioning, and we shouldn't do anything to affect their transition but it should be seamless with ours as well.

We don't want to be obligated by their rules and conditions, and we shouldn't feel that they should be obligated by ours, so it's discrete silos of transitioning.

BYRON HOLLAND: And I think that's an important point that effectively has been made there. There's an underlying assumption to where we were going with this, and that its focus is around the functions that impact us, as a community, not the RIRs or IETF.

STAFFAN JONSSON: If I understood well, there is a common understanding that the IP address and the protocol parameters are transitioning also. So, I think first step we should write that this is included in the transition, then maybe we could think if it impacts us, and if it doesn't impact us we don't talk about it. We go too quickly, I'm not sure that we are not impacted, for instance, by the IP addresses and the RIR transition.

KEITH DAVIDSON: I think we can capture a point on the Board that we need to take into account the other IANA database customers and their needs and transition plans.

BECKY BURR: Right. Take it into account and understand how their transition works and how it will affect us.

UNIDENTIFIED MALE: [inaudible] from .jp Before going into the content, can someone explain the meaning of steward or stewardship? It seems that the steward or stewardship is the keyword of the discussion, but I'm not an English speaker. I don't understand what steward is.

BECKY BURR: I think you understand very well, because steward is the key word and it's a little bit ambiguous. But I think that's a role in the way that we might talk about a trustee under RFC1591. It's helping to manage and preserve a shared resource for the entire community of users. But, really, that's what steward means generally, what we are really doing here is defining what that stewardship is. That's what the work that is here.

BYRON HOLLAND: So we want to have another question or two. The other thing is this is not a discrete process in a moment in time right now. We know we're putting something up that nobody has seen before. It takes time to soak it in, think about. Also, if you have that thought in the middle of the night, please feel free to send Keith an e-mail. No, feel free to send me an e-mail. You know, as a council we're also going to be thinking about

how we actually start to wrestle with this problem, so I'm sure something will be coming out shortly about a path for input.

But this is just the beginning of a process. We don't have to solve this right now, clearly, but if there's anything that we've missed, or anything you want to add, please.

PATRICIO POBLETE: Patricio Poblete from NIC Chile. I think that to better understand what's being discussed, I think we have to try to make a distinction between what's trivial and what's not. In a sense, there is a lot of this that is trivial. I mean, one needs to have an entity, like IANA, that makes the needed changes in the root zone. For instance, if we in .cl want to change one of our DNS servers, we need that to be registered in an efficient and competent manner.

But that's not rocket science. If it only was that we could understand why there was such a wide discussion process involving all the Internet community in the world, and the governments, and perhaps the United Nations, who knows, only to do that which is a clerical function, right?

That's the trivial part, and I'm afraid that sometimes we tend to get bogged down in that as if that was the important part, and it's not. Okay? So what's the important part for us? Delegations and redelegations. Who makes those decisions? Because once the decision is made, that goes into the root zone file and that's the clerical part. But who makes that decision?

So we need to clarify whether that's going in the same bundle with the IANA function, or if that stays in ICANN. Where is exactly that power of making those important decisions is for us? That's the crucial question.

If we could imagine an ICANN without the IANA, that might be an ICANN without teeth. They could make any decisions that they wanted but why would IANA obey those commands, right? If they are together it becomes automatic, but if you imagine a different contractor, we would have to have very clear rules about that.

So, my question is when the ICANN Board makes a decision to redelegate the ccTLD is it acting as ICANN or is it acting as part of the IANA function?

KEITH DAVIDSON: Yes. Point very well made, Patricio, and noted. I think when we get into our next session and start to see the tree of decision-making and structure, that might start to clarify what things could look like in various ways. So I think we're starting to get ahead of the game. Perhaps this is the opportune moment, unless anyone else has a really burning question, to transition to the second presentation?

BYRON HOLLAND: Sure. That would be great. Jay, come on up, please. So, the next thing that we wanted to walk through was just to start thinking about if these, arguably for the moment, are the gaps that need to be filled once NTIA pulls out, and some of them are technical or clerical. And then the fourth bullet point down there starts to talk about the more substantive

meaty issues, if everything in one house – everything run and done by ICANN – is one solution, clearly there's a spectrum of solutions that include full structural separation, and maybe even multiple bits of structural separation.

In a sense that's a continuum. Not only are those separate entities and organizations, but they can have separate impacts on accountability, trust, and oversight, and the interplay between the various functions.

So we thought it would be hopefully of interest, because some people have already started thinking about these topics, Jay being one of them – to just take a look at if the document we just saw articulated some of the roles and some of the gaps that need to be filled once NTIA pulls out, how can we start to look at them on that spectrum of potential solutions. This certainly by no means exhaustive. We heard some other ones the other day, but Jay is going to walk us through some of the work that they've been doing around trying to map roles to functions and structures.

Jay?

JAY DALEY: Thank you. I'm going to start just by showing you the straight text of the first two paragraphs of the NTIA announcement, just to follow up with Becky's bit there. The text is highlighted to make it very clear where the analysis that Becky has just provided for you has come from.

The first bit of highlight is the intent to transition key Internet domain name functions to the global multi-stakeholder community.

The second bit highlighted is the request for proposal to transition the current role.

Then they go on to talk about the role, and first, they're very clear it includes the procedural role of administering changes to the authoritative root zone file, as well as serving as the historic steward of the DNS. Now that's vital, as the conversation so far, as presented by a number of people within ICANN, has been solely about that second point there.

Then we have the third point, clearly, which is the contractual control that they have over the IANA functions and the cooperative agreement with VeriSign. Then, of course, the overall ambition of this is the privatization of the DNS. It's important to be clear that that's a very wider thing than any specific goal about ICANN; it's about the whole system moving in that way.

This diagram, which is impossible to see if you're not in the Adobe Connect room, I will try to make much bigger for you. The overview of functions, then, this is the oversight function. There are different interpretations of this, okay? So, this is an attempt at an interpretation.

We have the stewardship role. Now, traditionally the NTIA has promoted its stewardship through promoting top-level principles. I think we forget that the NTIA were, to a degree, very much responsible for the word multi-stakeholder, and the idea of multi-stakeholderism being a core part of Internet governance. They've also been very strongly behind the idea of a competitive market, and they've driven the particular phrase of "public accountability," and more recently

security and stability have very much become part of it. Now, there are other ways of wrapping up what the stewardship means. This is just an attempt to explain it.

Then we have the contractual oversight of issuing and monitoring the IANA contract, and reissuing, of course. And issuing and monitoring the root zone maintainer contract, that which VeriSign has.

Finally, there are the specific DNS root operations, where they authorize the changes.

We then move into, and this is going to be slightly tricky to show on the screen, the policy area. I just need to read this out for you. So, common to all areas of the policy we have monitoring the IANA SLA to ensure that it's actually delivering as required. Then we have the gTLD contract space, which is authorizing, contracting, and regulating gTLDs, authorizing, contracting, and regulating registrars (or gTLD registrars).

Then we move into the gTLD policy space here, which is setting the policy by multi-stakeholder consensus, and issuing, delegation, and redelegation instructions to IANA in line with that policy. So, the instantiation of that policy.

Then we get into the IP address and autonomous address space here. This is split into the two, because we have here the local policy, set by community consensus, where change requests are issued to IANA in line with global policy. And here we have the global policy, where delegations and redelegation instructions. So effectively, in the IP bit, that means this bit on the right, is the allocation of large blocks to the RIRs. On the left, it means that the RIRs handing out address space

within that, and occasionally asking IANA to change some name severs for their reverse lookup.

We get something very similar in the ccTLD space here. We have the local policy set within ccTLDs, and change requests issued to IANA in line with that policy, which effectively is us asking for name server changes or those things. Then we have the global policy here, set by community consensus, which is really just about delegations and redelegations.

Then, down here, finally we have the protocol parameters part of policy, which is setting policy by community consensus, and issuing change instructions to IANA. The final bit of the policy slide, here, are the IANA functions here and the root zone maintainer functions.

For the IANA functions, for all registries, their job is to:

- Operate the changes in line with published policies;

- Measure their own performance against an SLA;

- Refer complex or unclear change requests; and

- Where possible or allowed, publish all change requests (excepting, of course, that they get so many lunatic change requests that they need to filter out those.)

Then we have the specific DNS root operations that they do:

- Implement delegation and redelegation in line with policies;

- Check the changes are technically compliant (as the changes given by us country codes, for example, or TLDs); and

- Sign the root.

Then we have the root zone maintainer functions:

- Check the changes are technically compliant (the second pair of eyes to do that again, and that does occasionally throw up errors so it's not an unnecessary step);

- To publish the root.

Now, that's the policy makeup. I'm now going to show you some overlays. I'm going to make this smaller so that you can see them all in one go even though you can't read the detail anymore. The detail will hopefully be shown from the previous slide.

Here is the current overlay of organizational split. At the top here at the oversight layer we have the NTIA. Here, for the gTLD contracts and the gTLD policy bit, the global ccTLD policy, and the global IP address policy, we have ICANN doing that. I recognize that's through the ASO and the ccNSO, but the point is it's within the ICANN framework.

And here we have IANA functions operated on contract.

Then the other players that we have are for the local IP address policy, we have the RIRs in blue there, and then for the local TLD policies we have the ccTLDs. Down the bottom down here we have the IETF and the IAB setting the protocol parameter policy. Then finally we have VeriSign over here, doing the root zone maintainer function.

Now, one of the most interesting parts of this is the relationship between the IETF, the IAB and IANA. For the protocol parameters that are governed by the IETF and IAB, all changes come through a very clear specified mechanism, normally an RFC.

So we have full structural separation between the IETF, IAB, and IANA. Any change request made to IANA must go through a provable community consensus and must end up in a very specific published form. You do not get a random ICANN Board decision changing protocol parameter, basically. IANA has to respond to those in those ways.

The next slide, then, is this is the ICANN proposal they made last Friday to the SO and AC chairs. It is effectively an integrated ICANN, with ICANN having control of the IANA function, ICANN having control of the root zone maintainer function, having control of the oversight function. And within the detail of the oversight function we can see there are no longer any IANA or RZM contracts to issue, because their view is they get it forever and a day from that point onwards.

So we have other people who have made proposals as well. Another proposal came from the Internet governance project, Milton Mueller and [Brendon]. This has a very different structure. Did that not move? Right, okay.

So, at the top all of this oversight has gone and been replaced with a memorandum of understanding. Please don't ask me about that, it's in their paper. If you want more details, go and read that. There is a structurally separated IANA and RZM called the DNSA, which by its nature cannot do the second pair of eyes function, because you need

two organizations to do that – and there is a contractual relationship between them. But otherwise ICANN stays the same in that regard.

I'm going to show you some other options now, not because any of these are preferred solutions, but because it's important to recognize the scope, the space of solutions that may exist. One of the problems we have is people trying to limit where our thinking goes on this, and actually our thinking goes very broadly.

So one of them, the obvious one, is very similar to the IGP one. We have a new oversight entity here at the top. We have structural separation, and we have a new entity on the right providing the functions, so that this one at the top is a lightweight one which can decide whether either of the parties are doing correctly and replace them if they're not. Otherwise, it doesn't do much else. It's a constitutional president that many countries have, that type of thing.

The next one here shows ICANN in that top role. So, ICANN as the multi-stakeholder body is the one that maintains the principles, is the one that issues the contracts, and is the one that is responsible for the system underneath it. We then still have a new entity over here, doing the IANA and root zone maintainer functions, but we have a new entity over here doing the policy side of things, so that we separate out the oversight from policy by keeping ICANN in the big picture.

Then we have another alternative here which shows ICANN limited to the oversight and the gTLD contract management side of things. So, managing the SLA, managing the registrars, and the registry contracts.

We have a new entity that does the policy bit of it. We stay with the IETF and we have a structurally separated implementer over here.

Then, the final potential option – and you can design your own. If anybody wants to come up and draw I will do the diagrams for you. We could have 50 of these, I really don't mind. That's the point. We have ICANN as the entity that has the oversight and the contacts. We have a new entity here that does the gTLD policy. Us ccTLDs, effectively the ccNSO, becomes a standalone organization that has then the global policy control and we maintain our policy control at the lower level. The ASO becomes the NRO, which already exists so then there is a single policy across there. And the RIRs continue doing their work. And we have a structure separate entity there.

So you see, these are just a variety of different options that exists, and I'm sure many of you can provide more. There are some complex ones that people have put forward for the top bit up here being made by a committee of the great and the good, taken from the various different components underneath, which is just too many colors for me to show, but it's got some breadth to it, certainly.

BYRON HOLLAND: Thank you, Jay. That was very interesting. Everybody knew all of that, right? You could have articulated all the different roles? I mean, you are the biggest user of those services. Don't worry, I couldn't either.

Clearly, some people have been swimming in the deep end of the pool, and I think that was actually very, very valuable for us. So, when we talk about what is a steward, I think we started to unpack some of that and

then also be able to really clearly delineate the roles that are, in a sense, being pulled out of the equation.

I think that's very helpful, and I think, also, what Jay articulated, there are many different ways to skin this cat. Hopefully that's not just a Canadian expression. But there are many different ways to approach this where the technical functions, the clerical functions, etc. are addressed in a very safe, secure, and stable risk-free environment, while maintaining the accountability and oversight mechanisms. I think even those two words we need to parse, because they're different.

That is a great start on letting us start to think about what is the art of the possible here, given there is such a wide spectrum? I do just want to touch on something, because it's key to the start of it, which is what was presented to the SO and AC chairs.

Being one of the chairs that some of the initial stuff was presented to, I would say it wasn't presented as "This is the path that we are taking." There were many ideas which were shared which, without a doubt, there was an underlying bias towards a one-house solution. But it certainly wasn't presented as "This is the path." And I will say that all of the chairs in the room, it was a robust conversation, and the what was presented Monday morning was very different than what was being articulated Friday night.

So, there was a bunch of chairs who looked at the initial comments, myself included, that pushed back very hard on some of the key elements. And, to be fair, ICANN staff was listening and what came out Monday morning was quite different. But it still got an implicit bias to

kind of a single solution, without a doubt. I just wanted to make that clear.

So now that we've seen the articulated roles documented, the deep dive into what does that really break down like, and some sense of the possible in terms of solutions, one of the things that I wanted to do was as we approach this – and there's two pieces: process, and substance. I'm not going to treat it like church and state, and we can only do one or the other right now.

Let's have a dialogue about are there any principles that we want to put on the board for this community as we start to approach this subject, both in how we approach it (the process) and what we start to work towards come up with in terms of substance.

So, just start the thinking about this from a principles basis.

I just want to say Fadi has come in a few moments early, so welcome, Fadi. Thank you for joining us. You're going to get to sit in the messy business of multi-stakeholder conversation right now, so please have a seat. Don't let Fadi's presence color your views. Feel free to speak up.

Are there any principles that we should be thinking about? Think of the filter set through which we should view the process, challenge, or the substance issues. So just to get things going, in the CC community the notion of subsidiarity would be critical. That our local laws would be paramount, that we as individual CC operators would have to, as a fundamental principle, we would have to be governed by local laws before some global policy. Is that a reasonable principle through which to view it?

Don't all line up at the mic at once. Come on. I'm happy to walk around too, but feel free to use that. As we start thinking about these issues, how should be start to wrestle them down?

[Dotty]: That's already an accepted principle, and so I don't even see why it becomes an issue. I don't think it's being challenged in any way.

BYRON HOLLAND: I don't think it was being challenged, [Dotty]. I was just saying in terms of trying to give an example of a principle through which we should view how are we going to address the substance, that would be an obvious one. We're bound by local laws.

Are there any other? No one size fits all. Should we have a working group to wrestle with this in terms of process?

UNIDENTIFIED MALE: Thanks, Byron. I think the working group was a stretch of some sort for the ccNSO is inevitable obviously on this. I just think that a couple of primaries in view of this statement from NTIA that we should bear in mind. Especially if you read what's been released today and the move toward the multi-stakeholder based oversight and overall management process.

I think however we proceed, whatever the process is, there's a certain key definition, there's key things that you must clarify and define. One of them is what is multi-stakeholderism? Sometimes we talk about

these definitions and we take them for granted, that because you and I can [communicate] we all understand, but what about those outside? And also, do all of us inside the ICANN community understand what is multi-stakeholderism? That's the first bit.

The second bit is what is global multi-stakeholderism? Because these are words, and words are power. Lawyers especially will know, that when you interpret, for example, a law, you interpret it based especially on the words. Same thing with policy.

So what is multi-stakeholderism? What is global multi-stakeholderism? That needs to be defined, and it's more important because in different [inaudible] as you would know, whether through the ITU and other different entities, the very same issue of multi-stakeholderism is challenged or questioned. So it must be clarified in view of this development by NTIA.

Now, it's also important to also bear in mind that there will be questions from different quarters that will come about. For example, is ICANN itself the right forum of debating this particular transition? What NTIA has done, which is good, is indicative of how it would like to see the new ICANN framework, that it would like to see it being a multi-stakeholder driven process. But then, is ICANN the right forum to debate this considering that already ICANN is positioned to be the beneficiary, as it were, of this?

I'm not saying by that that we shouldn't debate it. No, we must be very vocal about how we see this happening, and I'm thankful to the presentation that Jay did, because it got me thinking that some of those

models are very good. Others leave questions. So then there's an integral of the ICANN community for us to debate this through our structures and say "This is how we say this." But there will always be questions about should this whole transition be debated within ICANN, or should it be debated outside ICANN. I think those are important primaries.

One caution, obviously, is this discussion substantially, in different quarters as well, may set ccTLDs against their own governments, because even at a local level the debates about whether ccTLD should a multi-stakeholder driven process, or should it just be a government thing.

I could just imagine a scenario in South Africa, where I come from, where we say "Multi-stakeholderism, Yee-haa!" and the government comes and says, "What's that? Can you tell us what is multi-stakeholderism?" So we can't help them, but we must understand that maybe our contributions as ccTLD could be a thin line to balance between what the ccTLD thinks is right, and what the government thinks is right. You know?

In closing, I think that part of the process now, of us considering this whole transition, especially from the ICANN community and from the cc community is – and I would imagine probably ICANN internally, in terms of management, are already considering that – this presents a good opportunity for ICANN, as well, to differentiate between ICANN as it stands now, and ICANN in the future, post this transition, as it would like it to be. Whether that involves your SWOT analyses and stuff, you know, but I think it would help to inform the discussion. Thanks.

BYRON HOLLAND: Thanks. I've got a comment from Keith, and then Jörg. I do just want to pick up just quickly on something you said, you know, the NTIA was pretty clear that it's ICANN's task to convene this discussion, so I think that's pretty clear. But the further point that you made was in convening it and potentially being a beneficiary of an outcome, we just need to be aware and conscious. What does that look like? What does that mean?

The other point that I think is critical to pick up is around the global nature of this. We have around 149 members of the ccNSO, we clearly represent the massive majority of CC domain names out there, but there's still another 100-ish CCs who are not part of our community here inside as a structure of ICANN, and how are we going to make sure that their voices are heard?

I personally think that we need to work closely with the regional organizations who can reach down into a whole other layer of CCs that we, just by definition of who we are, would be challenged to do that.

I want to certainly see how we can encourage the four ROs and our organization to find a path to answer some of these questions commonly. Not telling them what to do, they can ask whatever questions they want, but maybe at least we can also have a common set that we answer. Keith? So, Keith, and then Jörg, and maybe Lesley? Then Pierre.

KEITH DAVIDSON: Thanks. Just in concluding that discussion, I think [Vika] raised a very important point – and I just hope it's recorded on the board, it might not be, but I can't read it from here – but the principles of sovereign rights over ccTLDs versus the principles espoused in RFC1591 are clearly – I think that was a summary of something you said, but both of those sets of principles are very pertinent to this discussion.

Sorry, I wanted to interrupt the dialogue for the record to record that we are now joined by ICANN CEO and President Fadi Chehadé, and our two ccNSO Board representatives, Chris Disspain and Mike Silber.

Now that we're recording you in the room, could we have the courtesy of introducing ourselves as speakers along the way in case anyone wants to respond to specific questions raised by specific people? Thank you.

JORG SCHWEIGER: Is it really time right now for comments to the topic before or have we just moved on to another topic? Okay. Jörg Schweiger with .de Germany. Concerning the question about how do we tackle the problem, I'm in favor of setting up working group, because as far as I understand, there already has been a temporary working group being set up, so that could be very easily tasked with the a job that is to be done in the future.

To a certain extent, for example, it gives us some time to think about problems to not just be confronted with them but to think them through locally, to discuss them locally with our community, with our staff, with our governments, whatever. It removes the language barrier

that may exist as well, so I'm really strongly favoring any kind of working group to tackle the problem.

With respect to – and I just couldn't refuse to once again comment on the subsidiary because I think this is very interesting and crucial even for the design of the solutional space, I think we have to consider a subsidiary because for example within the presentation of Jay he was talking about local policy and he was talking about global policy. Very interestingly to recognize I think is that redelegation, for example, has been placed within the box of global policy. I would question that. Because once a string has been delegated, well, it's under our control. It's under the control of the cc. So why should it be up to any decision of a global policy maker? I just can't see the point.

BYRON HOLLAND: Thank you. Lesley and then Pierre and then we'll call it at that for right now.

LESLEY COWLEY: Thanks Byron. Lesley Cowley from Nominet.uk. Firstly I'd like to thank Becky and the team of wordsmiths for starting to define the scope of the conversation. From the earlier conversations this week, I think we were struggling to actually define what it is we're trying to talk about. So it's really helpful to start with defining the problem scope as it were.

That paper take us some way, but I'm still not crystal clear on what we're trying to solve the functional separation might be the answer to. We can get into looking at lots and lots of different models and

separation and so on. I think it would be helpful to explore further as we go what it is those different things might achieve.

The other more practical point I had was on subsidiarity. We're talking about local laws. Just to remind people that subsidiarity is also WSIS principle, which is very relevant this year as we're now coming up to WSIS Plus 10. That's talking about countries not being involved in decisions regarding another countries ccTLD, that's WSIS Principle 63. That's why ccs are quite difficult I think in this whole discussion because countries should not involved in decisions regarding another country's ccTLD.

BYRON HOLLAND: Thank you Lesley. Pierre, and then we'll give the last comment to you, Jay.

PIERRE BONIS: Thank you, Byron. Pierre Bonis, AfNIC, .fr. First of all, really thank you, Jay and thank you, Becky because it's really helpful. I think that the various proposals that Jay showed us shows that there are a lot of possibilities and this discussion opened a lot of options.

To come back to the question asked by Byron about the principles, I [inaudible] with subsidiary and the respect of local law I think this is interesting also to remind the principles that are common to all communities. Then we define the principles of ccs specially. As we try to apply principles to the process we can remind that the process should be open. The process should be done in a multi-cycled way and the

process should take into account the public interest, which is something that should be shared by all the community and all specificity is local and subsidiarity. That was my comment for now.

BYRON HOLLAND: Thank you, Pierre. Jay?

Jay DALEY: Thank you. I think it's important for us to note that nothing is being changed just because we want to. It's being changed because the NTIA is making a fundamental change and there are repercussions of that that need to be thought right the way through. Part of this process is going to be understanding what the problem is and getting an agreement of what the problem is before we can then move on to a solution.

One of the ways that I think about the problem is very much a risk - focused way. That's the nature of the job that I have to do running a registry. Some of the risks that have been already raised by people on the short list here that a failure of ICANN has a catastrophic systemic effect because it has become too big to fail because we have put all our eggs in one basket. That such a failure may leave the whole multi-stakeholder model discredited, that we may see errors introduced to the root zone file affecting all TLDs. Those are some large ones.

Then we get to some other ones that may see more towards the end of the spectrum that Patricio was worrying about. But an arbitrary instruction is issued to the IANA function (i.e. Something outside of

policy). Or the IANA unction makes an arbitrary change to a register on the outside of policy. There are a long list I think of risk that can be brought out. They need proper assessment, proper understanding. They need to be worked against a set of models to understand how each of those models can properly address those risks.

All I see so far in some of the presentations of models so far have been the risks. That's why for me this is an important way to tackle it.

BYRON HOLLAND: Thank you, Jay. With that, I am going to go to our featured guest today, Fadi. Welcome Fadi. I know there were some other questions. I'm sorry we'll have to take those as feedback. I'm sure we will have much discussion on principles in the coming days, but we do have a time limit to consider as well.

Welcome, Fadi. Thank you for joining us. Much appreciated. We've been having an interesting discussion about how we're seeing the question or the problem to be solved, so to speak. We've had very interesting dialogue here over the past couple of days. Kicked it off with Larry and Fiona presenting how they were viewing the question and their requirements so we got their first-person account of how their approaching it, what they're hearing and then also had the opportunity to question them.

We've had multiple sessions on different elements of this including having some big panels with the Chair of the IETF, Milton Mueller, and others who brought some very interesting perspectives, Pat Kane from VeriSign etc.

We've had some pretty fulsome dialogue here as we start to unpack this issue. As part of that, some of us have taken some stabs at putting pen to paper to really unpack our view of the questions and the spectrum of potential opportunities ahead of us.

With that, we wanted to just have Becky give you a quick run-through of what we initially, although it's still a work in progress, viewing the questions as. What questions are we answering? You can see it on this screen here if you can read that. Becky?

BECKY BURR: Thanks. This is just a work in progress. Throw up everything, look at it, see what makes sense. In the announcement that NTIA made it described its role as administering changes to the authoritative root zone and serving as the historic steward of the DNS. These two descriptions are really focused on the name functions, not the parameter protocols and numbers. So we acknowledge that there are other things there. But we just started to make a list of what it is that NTIA does. Obviously it authorizes changes to the authoritative root and importantly for this group, that includes changes that amount to delegations or to revoke a ccTLD delegation.

It oversees ICANN's performance of the functions in the IANA Functions Contract. It oversees VeriSign's performance of the functions in the cooperative agreement. It selects the IANA functions provider and the root zone management provider. It establishes through the contracting and the periodic rebid the requirements and specifications under which

those functions must be performed. It's not just doing the technical functions.

The IANA function contract, as you know, has requirements for documentation and response time and consultation and that kind of stuff. Then oversees ICANN's obligation to develop and implement consensus policies through a bottom up multi-stakeholder process as expressed in the Affirmation of Commitments and be accountable to all stakeholders. That's the sort of backstop role.

We're going to be spending some time in this community talking about each part of that and refining those things, but our goal is to come up with a collective view about what the USG currently does so we can know just what it is we have to be looking at and thinking about transitioning.

BYRON HOLLAND: Thank you, Becky. Putting you on the spot a little bit. I'll give you a moment to think about is there anything there that you think is a glaring error? Have we missed anything? Do you have any comments on it?

While you process that in the back of your mind maybe just ask you over the course of the week what's your sense of the state of play on this? Have you been surprised by anything? How are you seeing this issue evolving? What are the key hotspots or threats that you'd like to make mention to this community?

FADI CHEHADE: First, reacting to this the scope of the consultation will be published on April 7th, so I won't comment on it now. But we are listening to everybody. We are refining THIS. We're reviewing it with NTIA and on the 7th we will publish the scope as well as the process based on what we're hearing. If you have any input specifically on these things, please submit it. I think we still have that open until the 27th, which is tomorrow so at some point we can take all of this, synthesize it, produce what we think we heard, share it with NTIA, share it with the affected communities, the ISTARs etc. and make sure we're all in synch.

Then we'll publish it on the 7th for another round of public consultation. We'll have another yet chance for everybody to see because not everybody's obviously here. Everyone should have a chance to participate in shaping the process and so on and so forth.

I think what I'm feeling frankly is that this week has been extremely timely in many ways. The announcement of NTIA quite frankly was originally slated for next week. Then it was pulled up to the 17th of March. And it was pulled up largely for this so that this happens, precisely for this. There was no other reason. In fact, there were a lot of reasons not to pull it up.

But, we insisted that if they're going to do it they should allow our community to be together. And by our community I mean not the whole community but at least those who are here to start the dialogue and to discuss it. I think that NTIA was very wise to allow us this time. If this had happened in the absence of at least a gathering of this community, I think it would have been harder.

So I'm very, very thankful to NTIA for making that announcement when they did. It served us well. I see very productive dialogue and I think we will emerge from this week with some good ideas that will allow us to scope this and put a process in place that is acceptable.

The road from here to the end of the NTIA contract is long. We have 18 months ahead of us, but I want to say today again that there is no guillotine sitting in front of us at 18 months. If we do not have a proposal that we built with consensus in time for the end of that contract, I will be the first one to ask NTIA to renew the contract. There is no obligation for us to finish in 18 months other than we have a window, we have an administration that will change in the United States starting 2016, an election year.

There may be new people at NTIA. New people certainly in the White House, new people in the administration. Is it reasonable for us to say, "Let's try and work this out while the administration is still largely here?" I would say so. But it's up to us and we certainly shouldn't – none of us including me, starting with me, I'm committing to all of you – push for this change if we're not comfortable that we have a proposal that guarantees the things we all care about: the common principles of stability, security, openness that are all the things that NTIA put and in additional to that all the other things we worry about.

I would like to caution us from going down any paths that fragment the Internet. I think maintaining a single root with the registries of the Internet maintained as they have been faithfully for 15 years is an important goal to keep in mind. There are so many forces that wish to fragment the Internet. Now we have to do that with full respect for the

sovereignty and the independence of the ccTLDs as operators of their country domains.

We have to find that formula that respects both principles. The principle of one Internet, the principle of a single set of registries – because by the way there are entries into the protocol parameter registries and the numbers registries and the name registries that need to be coordinated. These are not distinct registries. That's why when NTIA was asking whether we should put all three under their contract at some point in the past, we kept them in one contract. There is a reason from an integrity standpoint to keep these together. Please, I beg us to be careful with the integrity of these technical registries.

The second point I'd like to encourage us to think about is that on the same day as the announcement of the NTIA, which you have on the screen (or parts of it), all the technical organizations issued a statement that was equally important to this statement in which they affirmed many of the same principles including the policy roles of the bodies that make policy, including the ccTLDs as well as the affirmation of the role of ICANN as the ongoing administrator of these registries. Do not divorce that statement from what NTIA did. In fact, they were tightly managed. One would not have come out without the other.

With all of this in mind we need to be very sharp with the focus of our public consultation. The public consultation is designed to ensure the accountability of those performing the work. That's the job. We need to give the world a sense that they are now replacing the U.S. Government in ensuring some of these things you see here on the bullets.

We need to find these mechanisms. Notice that when we drew that little slide, which is now on our website – the slide with the green bar on the right – we did not put multi-stakeholder mechanism or global mechanism or whatever across the whole column. We clearly divided it. We clearly separated the ccTLDs even though people may have said, as the IETF always says, you only have three registries names, numbers, protocol parameters. But we very specifically separated the ccTLDs.

This was thanks, in many ways, to Byron's guidance on this, that we need to all appreciate that there are some very specific things we have to do to provide accountability there that may be vastly different than what we would have to do for the generic names. There is deep appreciation that what we discuss as a mechanism, or set of mechanisms, to replace the USG role in terms of the accountability of IANA in performing your functions may be different.

Finally, I want to say one thing. If you pull up that slide again and look at it, there's some very important details. One of them is that you own the policies for your names obviously, right? I don't own the policies. What binds me to implementing your policies in the IANA registries – or the names registry specifically for you – is the frameworks that we've established with many of you.

With the other groups, the other rows for example today we agreed with all the numbers people that we will strengthen our agreements with them so when the world starts looking deeply into how are we accountable to them and to the world we'd have strong agreements.

Maybe we should discuss the same with you, maybe not. But we need to see how we can put you at ease that we are performing your functions according to your policies. One thought on that for example may be to fully automate any changes to the root as it relates to you and to give you, for example, a complete control over these changes so that no one can change anything as it relates to your entry in the root zone. By "your" I mean each of you individually. Without your not only complete acceptance but you will have a way to block that. You will own this change through a key or through some other mechanism.

These are the things that we need to strengthen between us independent of the public consultation. We have time to do this hopefully in the weeks and months ahead.

BYRON HOLLAND: Thank you very much, Fadi. Certainly I think there's some grist for the mill in the comments made there. I'm going to take the opportunity to open up the floor to my colleagues here if they had any questions or comments about what we've heard from Fadi because there's interesting ideas there. I know it's the end of two long days but we have Fadi in the room. You can get it straight from the horse's mouth. Now is the time.

UNIDENTIFIED MALE: Byron, are you calling our CEO a horse?

BYRON HOLLAND: Maybe while my colleagues are scratching out their questions I could ask you between middle of last week, seven days, how are you viewing the world today that is a surprise to you coming into it seven days ago? What are the big deltas from how you conceived where we were going to head versus where you've ended up today?

FADI CHEHADE: The way you formulated the question at the end is actually I'm finding that we are pretty much where we thought we would be. A little bit of shock in the community. I think we're experiencing that. Most people are a bit shocked. Two weeks ago there were some members of your community and other communities telling me it will be another 20 years before the U.S. even cedes on oversight. Only two weeks ago. Nobody believed they'd ever do it, but they did.

So in terms of your question, it is my expectation that the community would view this kind of where I thought it would be, yeah. Some people are upset with us that they were not briefed ahead of time. I had no choice. I was not allowed to. My board was briefed about 24 hours ahead of time. It's not like I had a choice. This was a tough negotiation.

The only surprise I have is in Washington. That's the only surprise I have. I expected Sarah Palin to say what she said. I expected various officials to say what they say.

But I tell you the biggest surprise I have in Washington. It's not that people are using this for political reasons. Politicians will do that. It's the lack of understanding of the multi-stakeholder model in Washington. It's incredible. It's really sad how little our own government officials in

the United States who supposedly should know this model in and out do not understand. So they immediately are reading Larry's announcement as he's handing this to the governments of the world or only to the governments of the world and reading all kinds of things in it that are false. I'm leaving out those who are politicizing.

Unfortunately, I was planning to take a few days off after this meeting, but I'm heading to Washington, D.C. There's multiple hearings now on the Hill, judiciary committee, various committees and I have been demanded as a witness.

BYRON HOLLAND: That's the biggest shock I guess on that front.

FADI CHEHADE: Yeah, I didn't expect the lack of understanding to be so deep.

BYRON HOLLAND: Keith?

KEITH DAVIDSON: Fadi, just picking up on that comment where you sort of alluding to the idea that the automation of the IANA function should proceed and so on. I think that triggers perhaps the difference in what becomes important to us and what's business as usual. For all of us now, the process by which we update our records in IANA is straightforward. We

have great reporting from IANA. Replacing a service level agreement in some form with someone else, somewhere else, is not so difficult.

The real gnarly issues for us – the real difficult issues – are the decisions that are made outside of our community. That is where there are delegations and redelegations. This is not when we are in control of our IANA entry anymore. While these are relatively rare things, certainly much rarer than they are updating the database, they are incredibly sensitive.

This is where the rubber hits the road. This is where you come across the direct conflict between sovereign rights and local Internet community rights and so on. So for us having a vehicle that allows us to know and understand it particularly in view of the U.S. Government's statement that this will morph to a multi-stakeholder model where governments must be equal players rather than senior players and so on. It's quite critical.

FADI CHEHADE: I'm so glad you said this, Keith. This is precisely what I'm trying to frankly save us from. If you folks take the processes you just mentioned and stick them into the green column, it'll be multi-stakeholder. Now I need to go explain to sovereign governments that we need all the stakeholders to decide on your cc's processes. This is why we kept that column on that side. And we said, "You tell us how you want me to do these processes with you. Let's design together in the absence of the U.S. Government how we want to manage delegations, redelegations, moving forward."

Let the green column be a multi-stakeholder column that provides some kind of an oversight that IANA is performing its functions according to its agreements with the constituents, meaning you. If we keep these things this way, I think we all get through this important tunnel safely. Rather than have the global community design how we will perform these functions for you. Let's do it for you, with you in a way that meets your requirements. Then let them design mechanisms to simply watch me perform them according to your policies and my agreements with you just like we're doing with the RIRs and the IETF.

BYRON HOLLAND: Thanks, Fadi. I have Roelof and then Annabeth and then Pierre and Staffan.

ROELOF MEIJER: Roelof Meijer, .nl. Fadi, did I understand you correctly that you said that there will be a consultation – no a draft, scope of the whole thing will be published on the 7th of April? Is that going to be published by ICANN, so not by the NTIA? Does that mean that ICANN community's going to determine the scope?

FADI CHEHADE: No, it's based on what NTIA has told us. Clearly there has been some confusion in the community so we're going to clarify that with NTIA and publish it. We will clarify it with NTIA and publish it on the 7th of April.

ROELOF MEIJER: My second one is more of a plea, and it is to keep absolute focus on what it stipulated in the communiqué of the NTIA, the role that the NTIA is playing now. We will be very tempted to tweak certain parts in the structure that we have now and I think that's a very bad idea, mainly because we're going to lose direction, we're going to lose speed and we're probably not going to finish this whole thing in time. And the world is watching. Maybe not the whole world but at least those that are interested and have something to say about it are watching if this process is going to work. Some of them will be ready to jump in if they conclude that it's not.

One of the things I've been hearing already and I've just heard it again yet now is, for instance, this very sensitive process about redelegations. It's not the NTIA who's doing that. It's not the NTIA who is making policy on redelegations. It's further down in the tree. It's not the NTIA's role to execute redelegations. I think within the ICANN organization and community, we make the policy.

Although I know I'm in the lion's den when I say this but I think we should talk about it. It's the oversight of also that process but quite a few other processes as well.

UNIDENTIFIED MALE: Maybe we are the only two then.

CHRIS DISSPAIN: Byron can I respond?

BYRON HOLLAND: Just one second, Chris. I don't often get to shut Chris down. Just enjoy that moment. So anyway, I just want to make note of the fact that we have Annabeth, Pierre, Stephen and Nigel so the queue is forming quickly. I'd also just like to say, I have heard those folks speak from time to time before. If there's anybody else who would like to jump into the queue, I'll put you in the front of the queue or wherever you'd like to go in the queue. Please anybody else most welcome to join the conversation. Very short intervention, Chris.

CHRIS DISSPAIN: Only just to say that I think the keeping it simple is actually the key to this. We are in control to a great extent. The scope's going to be provided. If we live within that scope and get what we want within that scope, then once it's all over and we've moved on to the next stage if you want to pursue the next aspect of it, etc. that's fine.

The only other thing I really wanted to say was critically importantly don't forget the work of the framework of Interpretation Working Group has been put in place – I know it's not finalized yet but almost finalized – which really does provide you with the meat and vegetables of the redelegation and revocation, delegation stuff, which has got nothing to do with U.S. government's roles.

BYRON HOLLAND: I just want to make the point too that Fadi was booked here till 3:30. We'll keep talking while you move your appointment. Annabeth?

ANNABETH LANGE: Hello. Annabeth Lange here from .no. I would like to come back to the form that you showed us, the slide you showed us with the green thing on it. It would actually be a good idea to have it here while we're talking about it.

I really think it was a good idea to have it in four sections to divide it between the protocols and the numbers and two sets of names. But on the right column, it was written multi-stakeholder for all future thing. It was set up what is the situation today for the oversight. Then the way I and a lot of others, which I've understood from the questions, I've understood that multi-stakeholder isn't in the right column. Was it that should be where the result not those who are going to discuss how we end. You see the difference? I think it might be clarifying for some that it was more like a question mark in that column.

FADI CHEHADE: I'll make this very easy. I actually I'll admit now publically, I didn't want the word multi-stakeholder there at all because of [inaudible].

ANNABETH LANGE: Exactly.

FADI CHEHADE: But the U.S. Government kept saying, we're worried that people misunderstand. So I told them “But the ccTLDs may not have.” You just helped me by giving me very good exit from that. What we're talking here about is the result, not how we get there. How we get there may

be a government that has sovereign rights over these mechanisms of accountability. I'm with you on that. I think this helps me quite a bit.

ANNABETH LANGE: Okay. Thank you.

BYRON HOLLAND: Thank you. Pierre next.

PIERRE BONIS: Thank you, Fadi, for having shared this information about the public consultation that's coming to be issued on the 7th. One question about that. Don't you think it's going to be difficult to explain to people who have submitted already a lot of papers through NETMundial before the decision of the NTIA?

And talking about U.S. government oversight on the NTIA's function. A lot of contribution like NETMundial was talking about that because it was before the announcement of the NTIA. Don't you think it's going to be difficult to explain then that they have to rewrite something once again in such a short time?

FADI CHEHADE: No, we couldn't ask this of people obviously. Leave NETMundial out for a minute. What we will put out on April 7th is nothing but a summary or synthesis of everything we heard this week plus all the people are sending now via e-mail because we have an e-mail link on the site so

people are sending ideas. But it's all about process, not substance. It's entirely about how are we going to manage this, folks. That's it. It's purely about process. No substance yet.

Once we get the process nailed – and so we'll put this out to simply say give us more input. More input on process will open it. By the way, today at 4:00 I will be asking the Government of Brazil at the request of NTIA that we take 90 minutes during NETMundial to discuss also the process.

All the participants at NETMundial who are anxious to go and talk about IANA tell them, "Look, we have a process. It's already started. Do you have input? We'll take some more input from you at NETMundial." We'll have a 90 minute window in NETMundial. I hope I clarified that situation.

BYRON HOLLAND: I think that's good. We have Stephen and then Nigel. And then we probably need to respect Fadi's time on this, and actually our own time, and wrap it up there.

STEPHEN DEERHAKE: Stephen Deerhake, American Samoa. If I could, Fadi, I'd like to go back to the answer you gave to Byron's question in which you expressed surprise at the reaction beyond the usual suspects that you've seen so far from Washington. Frankly, I'm surprised that you're surprised because this tells me that you are being ill-served by your advisors, who fail to appreciate just how functionally unfunctional Washington is.

I suspect that you're going to see a lot more pushback including pushback from both sides of the aisle going forward on this. Precisely with the know-nothing crowd, the "Oh my God, Obama's giving away our Internet." My question is: is ICANN prepared to engage in the educational and lobbying effort that it's going to take to overcome that.

FADI CHEHADE: I certainly appreciate what you said. Maybe I was showing more frustration than lack of knowledge but I'm deeply frustrated by what you said. Yes, we have started a pretty extensive lobbying effort about a month ago. We've always had access to members of the Washington political class, but we have increased that effort now.

More importantly, we're now working with other members of the community more closely including key players that have more effect and dollars in Washington than I will ever have. You saw the very positive statement from Verizon, very positive statement from Microsoft, very positive statement from AT&T, very positive statement from Comcast, and on. These are the guys that need to step into D.C. and say, "Look, what's wrong here? This is good for business. This is businesses and U.S. Government stepping out of the way of businesses and letting the world manage this growth.

The answer to your question is yes. There's quite a bit of coordinated effort. I'm spending the whole week, next week. One example of it – are you back in D.C. next week? On Friday morning one of the most Republican think tanks – the Hudson Institute –agreed to do a very important seminar in the morning that I will be speaking at along with

some of the top republican thinkers in Washington. That's an example of multiple things we're doing in D.C.

BYRON HOLLAND: Thank you, Fadi.

KEITH DAVIDSON: Can I intervene very quickly there, Byron. Stephen I think good comment. In fairness to the staff I think we have a very good team. I think the team advises Fadi well. I just think Fadi by his nature expects the best out of people rather than the worst. His surprise may have been at human nature rather than because he wasn't adequately advised.

BYRON HOLLAND: Two more questions. We have Nigel and then one from Adobe Connect. Nigel, in the interest of time, an economy of words please.

NIGEL ROBERTS: Economy was what I was working on. I appreciate Fadi's time here on this. What's important for a customer of the IANA services everything ICANN does for the ccTLDs is consistency, accountability – and here's the key: redress if something goes wrong. There's been in the past a lot of unwise and misconceived decisions by ICANN in relation to ccTLDs. I'm not here to disinter those, so it will be economy of time.

The ccNSO that you're here today is the very embodiment of forgiveness. I think that shouldn't be underestimated.

What I want to ask about is this. And it's a yes or no answer so you can either answer it yes or no or you can give some comment is that in any proposed structure will you ensure that there will be a redress facility based on something that is predictable and reliable, a judicial function if you will that's based on respect for fundamental rights as we understand them in the world?

FADI CHEHADE: Yes. And to show you it's a real yes, read in detail the statement that we got out with the ISTAR. You will find in the fourth paragraph a very clear section for the IETF that says if the IETF is not satisfied with how we implemented their policy, they can come to me after they talk to staff. If I fail, they can go to the Board. And if the Board fails, they have redress outside the board to a new mechanism. Absolutely.

This is what I mean by saying let's strengthen these things between us and let's give you all the redress and the support you need so when the world starts saying "Oh, we want to watch over how IANA is performing," we can show them what's in place.

With the RIRs we agreed we're going to move forward in fact as fast as possible between now and June to start showing the strengthening of these things. I invite you to do the same with us either as a group or individually. I'm here for that.

BYRON HOLLAND: And I think the final question goes to the chat room.

UNIDENTIFIED FEMALE: Okay. Javier Rodriguez is asking: “seeing all these global changes, how intense will the wave of change in the ccTLD arena be? Does multi-stakeholder models in some ccTLD raise huge waves?”

BYRON HOLLAND: I think that's actually more a ccTLD general question than a question for Fadi. So maybe we’ll – sorry to that individual right now. We'll park it for the time being.

FADI CHEHADE: My general answer to him is let's reduce the anxiety. Let's do things calmly. Let's address the needs we have calmly. As I said before, there is no pressure other than it's an opportunity. Let's take the opportunity and let's make the most of it. To those in Washington who don't believe our community knows how to solve this on its own, let's show them otherwise.

One way to tell people to back off is to show the multi-stakeholder model works. We listen to each other. We support each other. We strengthen our agreements and we're accountable. Please join us in this journey.

I want to say one last thing. With the help of Chris and Silber who have been very good guides for me, certainly as was Byron in the last few months, I want to tell you that my understanding personally of your

needs and how you work has grown tremendously. I have deep respect for your work, for your independence, and I'm here at your service. We are at your service, period. We are not here to control any outcome. This is your outcome. Please define it and come to us.

I will do everything I can in the next few months to come and visit not just me but my staff to come and visit all the ccTLDs as much as we can either regionally or in countries so that we can listen also to your input and strengthen our support for you. Thank you.

BYRON HOLLAND: Thank you very much, Fadi. And to Mike and Chris for taking so much time with us. A very interesting discussion. Let's thank the three of them in the way that we normally do. Thank you, gentlemen. And with that, I'm going to turn it over to Keith to wrap us up.

KEITH DAVIDSON: And I think also we owe a vote of thanks to Becky and to Jay for the work they've done in preparing this particularly difficult subject for us. Can we join in thanking them both?

And apologies to allow this session to run over time. We are 18 minutes late, but it's an unusual opportunity that we had to put our Board members and Fadi on the spot. I do hope that it has given us more information and more questions than answers at this stage.

I think we're now going to a tea break and then at 4:00 the ccNSO Council is meeting back in here. Sorry that this impacted adversely on your tea break but would all the council be back in the room at 4:00

sharp. As always ccTLD members are welcome to attend and observe. Thank you.

[END OF TRANSCRIPTION]