LONDON – ccNSO Members Meeting Day 1
Tuesday, June 24, 2014 – 09:00 to 18:00
ICANN – London, England

BYRON HOLLAND: Well, good morning, everybody, and welcome to London, the ICANN 50 meeting. Hopefully you've been able to enjoy a little bit of the good weather in London, which isn't always the case. Anyway, as always, we have a packed agenda and the Program Working Group has definitely structured a very interesting two days for us with a lot of very substantive sessions.

I do have a couple of housekeeping notes. One is just a reminder for those who have presentations that they need to have loaded for whatever session you're participating in, the goal is to have those presentations to Gabby and Kristina 24 hours in advance. So if you have been a little bit negligent, please get them to Gabby and Kristina as soon as possible. And on another note, please make sure they're the final version that you're sending. Thanks very much.

Before I hand it over to Katrina to walk us through the program, just a reminder that we have the meeting with the Board at 9:45, and it's on the third floor in this building. So I think we can walk up to it. It's on the third floor. And again, that's at 9:45. So the first session will end at about 9:40, and the we'll have to make some haste to get to the Board session at 9:45.

So with that, again I'll just say welcome to the London ICANN 50 meeting and pass it over to Katrina to say a few words from the Program Working Group.

KATRINA SATAKI: Thank you, Byron. Good morning, everyone, and I'm very happy to see so many of you awake and ready for two interesting days here in London. On behalf of the Program Working Group, I'd like to walk you through most interesting aspects of the agenda. Of course every presentation is going to be interesting, I'm sure, but there are still some things I'd like to highlight before we start.

First of all, again we have a lot of discussions regarding Internet governance. So this, for example, today we have Internet Governance Session 2, a very interesting panel. We have interviewers, Matthew and Becky, from our community. Then we have great panelists who will share their views on the perspectives on enhancing ICANN's accountability process. And you know that accountability is a very hot issue, going to discuss a lot these days.

Then tomorrow we have another session on Internet governance. It's on IANA stewardship transition accountability. This session will be moderated by Byron, and really would like to invite all of you to be here and participate because your views, views of regional organizations, are very important because we're going to talk about the selection process and how we're going to proceed with stewardship transition.

Another interesting session will wait us tomorrow. Tomorrow morning for the first time we have this four-month registries versus registrars. So we invited registrars to share their views and to talk about their problems, what problems they have working with ccTLDs, and at the same time we can tell them why we're not happy with things how they want us to be.

Of course those are just highlights and we have many other interesting sessions including a session on security, legal and policy. And of course traditionally one of the most interesting sessions, ccTLD news.

I'd also like to remind you that we have set up an Adobe room. If you go to the ccNSO website at ccnso.icann.org on the first page you can, first of all, access agenda. That's what I'm talking about now, and you can see full agenda. And you can have, by clicking on Adobe room, ccNSO Members Meeting Day 1 and Day 2, you can access the Adobe room. Just enter the room and participate in discussions. You can ask questions. Just fully utilize this possibility to use Adobe room.

Of course I must mention the most important event that's tonight. We have ccNSO cocktail. It's not far from here. It's walking distance [inaudible]. And if you enter it in Google, you'll see that it's advertised as modern child-friendly option with views. I'm sure it's ideal for a ccNSO cocktail. [inaudible]

Of course have to thank all our generous sponsors for making this cocktail possible. So thank you very much. It's really a very important socializing opportunity to talk in not-so-formal environment is a really very important aspect of our meeting.

So I'd like to welcome you to the ccNSO, and without further ado, I would like to start with the first panel and invite Patricio and the three panelists to the stage and start discussion on two-character domain names. That's something that emerged last minute, and since there was an interest triggered in the community, we decided to squeeze this panel into our agenda, because apparently this was an important issue. So the floor is yours.

PATRICIO POBLETE: Thank you, Katrina. Please I'll invite our panelists to come here. Okay, with that, Jörg, Lyman, and Daniel to be able to participate in this impromptu session. It was added very late, but I think it's important. Well, listening to some of the feedback that you are giving us after the meetings, I think I'll try to [inaudible] and go for a standup comedy instead of just sitting here.

The topic of this session is the introduction of two-character domain names in the new gTLD space. This is motivated by a request from several of the new registries for authorization from ICANN to use some [subset] of the two character domains at the second level. The rules are that those two character subdomains are usually not allowed unless either there is an agreement with the corresponding country code manager or with a related government, or by approval from ICANN.

Now, the requests are of several different kinds. In a few cases, what's been asked is for the release of two character subdomains that are unassigned that currently do not correspond to any valid country code. There is also a request from .wiki for two character codes that actually identify languages rather than countries. But in some cases, there is an overlap. There is [coincidence] with two character codes that happened to identify both languages and countries.

And there is also a request from .global, which I think [inaudible] coincide with country codes because it's for two character strings that are non-alphabetic, or at least one character is non-alphabetic, like number and a letter. So that's the context.

And there are reasons for approving this kind of a request and there are also reasons for opposing it, so we have a panel that probably will speak for both sides.

We don't have a lot of time, so we'll just begin the panel. But before doing that, I will ask you to use your cards. I would like to know which of you and your respective registries do allow two character domains that may coincide with country codes. The green cards, please. Yeah, okay. Thank you very much. I see Eduardo Santoyo here. Colombia is very popular as a second level domain for many of you. Yes?

UNIDENTIFIED MALE: [inaudible]

PATRICIO POBLETE: I'm not exactly sure. I think we're talking about the second level unless somebody corrects me. I think it's second level. How many of you disallow two character strings that may coincide with country codes in your registries? The red cards please. Just a few. Which of you just don't care? [laughs] The yellow cards.

[inaudible] Lyman may have to leave early, so I'll offer him first opportunity. He was with RSTEP. I think he can tell me exactly what the acronym means. They have done studies and recommendations that have to do with this. Please, Lyman.

LYMAN CHAPIN: Thank you. RSTEP with the "T" is the Registry Services Technical Evaluation Panel, and it's part of the RSEP without the "T" which is the

Registry Services Evaluation Process that is managed by ICANN staff. I will try to keep this short and as relevant to the issues that are of concern to the ccNSO as I can.

The reason that I'm here is that RSTEP conducted a review in 2006 of a request from the .name registry to release – or not to release – but to use two character names at the second level. In a program that they wanted to offer, their model is that the second level is a name – a proper name, a personal name – and then registrations at the third level are offered by the .name registry directly. So .name does not allow people to register at the second level. They offer registrations at the third level and the second level is shared by all people, for instance, with particular surname.

And they were particularly interested in names like Mg, Li and surnames which are common two character surnames in different languages and different countries.

What we found – and the reason that this is perhaps interesting – is it points to the difference between the way in which names are allocated in country code TLDs and the way in which they look like they may be allocated in gTLDs. The current request from six different applicants would affect a total of 148 gTLDs.

And so we have an issue that's similar to many that we've uncovered in the New gTLD program, which is that the scale of an issue actually affects how we think about it so that when things are relatively well contained as they were with .name in 2006, the analysis was fairly straightforward. It's very possible that as that expands dramatically from one gTLD with a very limited scope in its offering to a much larger

set of gTLDs. Some of the issues may change, but I'll give you a sense of the issues that we looked at in 2006.

We examined in order to determine whether or not there was a security or stability issue with the .name proposal, we looked at the general case of domain names that end in tld.tld. And we had, through the generous cooperation of Nominent, we had access to quite a bit of data from their experience with co.uk, ac.uk and so forth. Many instances of two character names at the second level deliberately structured – not randomly assigned, not just sort of handed out to anybody who wants a two character name, but deliberately structured to create subtrees under .uk that had particular meanings.

We found a number of things. We found that from a technical perspective that there was no problem that we could find with having two character names at the second level, and we found in particular that the folks at Nominet had not encountered any particularly important problem with the way in which two character names were used in their subtree structure.

At the time in 2006, search list processing had just emerged as a common feature. In particular, web browsers, but of other user interface software as well. And we examined the way in which search list processing could create a confusing situation in which either in the case of a domain name that ended in tld.tld it was quite possible – at least in principle – to erroneously resolve either the name ending at the end of the first TLD (in other words, not properly appending the final TLD), or conversely, a name that was intended to resolve at that first TLD erroneously having the second TLD appended.

In either case, you could end up resolving not the name that the user intended, but a name that was created as an artifact of the way in which search list processing happens when you type something into a URL bar, for instance, in a browser.

But although we found that this is something that could happen in practice, we found almost no instance in which it had actually occurred on anything other than a tiny, tiny scale in reality. So we found very few practical circumstances in which that had created any problems.

The end result of all of this was that the review panel that conducted the RSTEP review of the .name request found no threat to security or stability, and we gave essentially a green light to the .name folks and ICANN, in turn, with their RSEP process turned around, and as you know of course, approved the .name application.

In the current circumstance, I went back when these applications came out, they have not been referred to RSTEP for review. The six applications are still in the RSEP process and ICANN staff have not asked me as the chair of RSTEP to conduct an evaluation. And this is of course primarily because none of us, either staff or myself, going back to the 2006 review, have found any reason why the conclusions of that review should not apply to the current case.

The only thing that seems to me to be potentially different is the much greater extent to which search list processing is involved in the construction of domain names that actually get resolved today. And I raise that only to point out that I have gone back and revisited the arguments that were made and the conclusions that were reached in 2006 and have found no reason to doubt or reopen any of those.

So the only thing that I can imagine that would change the circumstances in 2014 as opposed to what obtained in 2006 would be the possibility that the broader use and more widespread use of search list processing might raise the level of concern that these kinds of confusions could occur.

I'm leaving aside for what I hope are obvious reasons the potential for user confusion. The potential for user confusion is and was in 2006 – well, much more so than in 2006 – is enormous. But we bought into user confusion as soon as we decided to have a New gTLD Program. That was not my decision and it's not something I'm prepared to talk about. User confusion is going to be everywhere. That's not an RSTEP issue. The "T" in RSTEP is "technical." We don't get into that. Thank you for the opportunity to make those points.

PATRICIO POBLETE: Jörg, please, if I understand, you have [inaudible] slide in this panel, the only slide.

JORG SCHWEIGER: Yeah, if you can just bring it up. Masterfully crafted last night. What's going to appear on the screen, I think I wrote a comment on the ccNSO list that initially sparked this discussion. What I wanted to do with that was just to raise awareness just to discuss and indicate the potential risks we encounter as a community if we leave that uncommented. And I think there was a risk that we just do not talk about it.

The implications that I do see is that we would agree to a precedence. I'm going to walk through without it, I think. If you could just push [inaudible]. Yeah, there we are! Okay, that's the main message.

We would agree to a precedence where we would end up – or might end up in the future – with a general right for new gTLDs to register any two-character domain names under all of those gTLDs.

Given that, what is the implication for us? I think that would surely strengthen the market position of the new gTLDs. And it might, as we heard, lead us to some technical [inaudible] of traffic. It might lead us to some user confusion. And I was just wondering whether or not the corresponding RFC which is 1535, I think, is still valid or not.

What I just wanted to do is raise your awareness, try to discuss if we want to pass that [uncommented], which would lead to generally two-character domain names for all new gTLDs. If we would want to comment and just to steer the discussion into a different direction.

By the way, I'm absolutely the wrong advocate for the problem because, as I've been indicating before, we do have two-character domain names under .de and I'm talking out of experience.

So referring to this generally allow two-character domain names precedence, that's exactly what happened in Germany. So you might know that there had been a ruling from the federal court that Germany or that the .de registry needed to register Volkswagen and they got an abbreviation that is vw and we were forced to register this two-character string. We reacted to that by opening up all of them because

we wouldn't want to be confronted by lawsuits all over the way just to register each and every one.

So we've been doing exactly that. We've been registering all of those. And I fear that leaving this uncommented, we would just agree to a second step, and that second step would be opening it up to the [inaudible] space. And that is basically my point and I think we should discuss whether we want it or not. And I do have some options in mind. What we might want to do, but I don't want to steer the discussion from this place [inaudible] involve you. Thanks.

PATRICIO POBLETE: Okay. Daniel?

DANIEL KALCHEV: Okay. So we already had the good presentation by everyone, which was very to the point. More or less, the essence of what has been said, with the exception that I think that the evaluation that was done in 2006 regarding the .name application and the possible implications of the tld.tld search pattern is very different from what will happen when this is [evolved] in the gTLD space in all gTLD domains.

The reason this is so is that in the .name case, most of those domain names are not used for anything else than the websites and e-mail. They usually don't host their own hierarchy of competitor networks, no subdivisions and the most dangerous form of this search problems would actually never happened.

So in this regard, I would urge RSTEP to do the same investigation again in the view that in the gTLD domains, those two-letter delegations will have further sub-delegations. Some of those sub-delegations may happen to be malicious in a way for one purpose or another. So the end result of this situation is just [worth qualitative] service.

The thing is it is not worth [qualitative] service for the gTLDs. That would be their problem. It may turn out to be worth [qualitative] service for the ccTLDs because the name we registered to our applicants, they maybe replicate it in some other hierarchies and they may end up being spoofed through this search process. Or maybe they're, for example, sites or whatever will end up being spammed with much more requests that they would expect coming from some other places [inaudible] and so on.

So I don't think we can stop this or we can prevent this in a more general way. And in some sense, I think that it may be better to allow it actually. But have a discussion on it because this will prompt the different software vendors to improve their software and reduce the chances of this happening. If we just let this happen quietly, things will be bad in our opinion.

PATRICIO POBLETE: Thank you. Okay, so you've heard some arguments. I would like to hear now from you. What do you think? And what is your experience with it? I might ask Eduardo, for example, to tell us if it's ever been a problem that "co" is such a popular second-level domain in many ccTLDs. Can you say something about that?

EDUARDO SANTOYO: Really since the very beginning we realized that two characters has many meanings for many things, not just in the domain name space. For instance, in our case, .co has been used in the domain name space as a second level in many countries in the country codes to refer to commercial activities or companies. But it's also used many years ago from the industry to say that it's a company, mainly in the U.S. or U.K., for instance.

Of course it's also a country code for Colombia, which [pretends] or tries to identify the country of Colombia. Since the very beginning of the domain name in Colombia, we have to live with the reality that .co has been used for many other users from many other countries in many other places. We need to live with this reality since the very beginning, so it's not an issue for us. It's something that we needed to deal since the very beginning.

And probably to understand that having these different meanings of the .co extension or the .co combination of characters what we need to do is make a stronger efforts in order to make the people know that .co is our TLD. It's not a second level. That's it.

PATRICIO POBLETE: Thank you. Gabby has the microphone if anybody else wants to say something. Over to the back.

SIMON MCCALLA: Hello. Simon McCalla from Nominent. I just wondered what the panel thought or if they had any thoughts about the impact of Mozilla's public suffix list and the effect that can have on making second-level registrations look like a registry in terms of user confusion.

For example, we've seen mistakes made in the U.K. in the pubic suffix list where domains have appeared to look as if it's possible to register third levels underneath them or vice-versa, and the browser will display the most significant part of the domain name. So Firefox does this. For example, it bolds the piece of the domain that's been indicated in the public suffix list, so it can lead to user confusion. I wonder if you just had any thoughts or considerations of that.

PATRICIO POBLETE: Any words on that public suffix list?

JORG SCHWEIGER: Yeah. The issue of the use of the public suffix list and the more general question of – I forget the term that's currently being used, but general applicability. Again, I forget the term. This is an issue that we have dealt with on a small scale already in many environments, including the one that Eduardo just mentioned.

What is changed is that the scale and the scope of the problem is suddenly expanding. And as Daniel mentioned just a moment ago, that may very well change the way we look at it.

When you have a relatively small problem and it's being dealt with in an environment in which people are making good faith efforts to try to

make sure that things are interpreting correctly, that's very different from the more or less free-for-all environment that we're possibly looking at with the new world of many, many, many new gTLDs.

It won't be possible, even with good faith on all sides, it won't be possible to exercise the same kind of control that we have in the past. There will inevitably be circumstances in which the way in which two-character strings – not just two-character strings – the opportunity to try to spoof or scam or otherwise confuse users are going to be vastly greater than they have been.

But particularly in the case of two-character names, there will be circumstances in which they are used at the second level within new gTLDs that create problems for users that we haven't encountered before. It's clear that the scope of the problem will become greater.

The question is whether we can do anything about that by limiting or restricting the way in which two-character labels are allowed to be deployed at the second level. The difficulty there of course is that we have a wealth of precedent for allowing those strings to be used as second-level labels and trying to come up with a new scheme that respects those precedents, many of which have been in widespread use for a long time, but also creates new boundaries for new gTLDs will be a very difficult enterprise. I'm not sure how we would even go about doing that.

PATRICIO POBLETE: I think we have very little time left, so [inaudible] goes to Manuel and then Annabeth.

ANNABETH LANGE: Annabeth Lange from .no, Norwegian registry. I'm not the right person either, because we opened up in 1990s – actually very early. But we have regretted it because we have had problems – a lot of problems. We even had a court case about it.

The biggest problem was .co [inaudible]. Yeah. The one that registered .co.no as a registrant, he started a registry and sold it as the same product [inaudible] .co.uk. So they kind of stole our identity. And since it has to do with the country, it might very easy confuse the users. So they thought they bought a Norwegian name under co.no and that it was a Norwegian registry and Norwegian rules and everything, but it wasn't. So I'm kind of uneasy. It's not [inaudible] say go ahead. It might easily create problems.

Certainly in that extent – and I agree with Danny – that .name is one case, but this is 1500. And if we open it up, we can't restrict it and say, "You can and you can't." Either we open up or we don't. And also the suggestion, I read the papers coming in, some of them suggested they should keep away from [inaudible] list but they can use the rest. But either all or none, because it might easily be new countries. So either it's country codes or not.

PATRICIO POBLETE: Please, some very short remarks.

UNIDENTIFIED MALE: Okay. So I'm about to actually give an example very similar to what I was going to say. In the past, we had a case where somebody has come in contact with the holder of bg.com, some American company. They got an agreement that they will be allowed to register domain names in that space.

So what they did was come to parties in Bulgaria and claim they are the registries, where people need to register their names and it looks much better to have a name something.bg.com that something.bg, for example.

That was short-lived, because I think the American company got smart about it. It didn't want to get involved in this. But the precedent is still valid. I'm absolutely sure we will see this thing in the gTLD space if two-character domain names are allowed.

PATRICIO POBLETO: Jörg?

JORG SCHWEIGTER: I would answer to Lyman or make some amends. You've been saying that the [inaudible] is minimal. To a certain degree, I would agree to that, even though in the case of vw, we've been conducting some – we've been gathering some – data an there wasn't a single second where there hasn't been traffic that was not intended to go our way, but did. So it is a problem.

Still, we live with that problem. We've got many cases. We've got .name. We just heard about that. We have [CentralNIC] who was selling

cc.com all over the place, so we do have the problem. I'm aware of that. But the question would be if we would leave that uncommented, would we encounter a situation where the problem is going to get worse or not. I would be just glad to take a closer look at that to make sure that we do not end up in a situation which we might not want to handle. I do not feel, by the way, that we are creating boundaries, but what has been done is that those boundaries already have been created by ICANN with the RAA.

What we are supposed to do is we are supposed to open up those boundaries and that has got to be a process that is well-understood. And for that, I would command an RSTEP project to look further and more detail into potential problems.

PATRICIO POBLETE: Okay. I think we should be with the Board in about two minutes on the third floor. So before we do that, a final show of cards. After hearing all these arguments, how many of you will say that two-character domain names should be allowed in the second level in the new gTLD space? Green cards, please. Should they be allowed? Okay, thank you.

Red cards, shouldn't be allowed. Red cards. Okay, just a few.

And the yellow or orange cards. Some of them should be allowed, like they are being requested actually this time. Okay, thank you very much.

[break]

YOUNG-EUM LEE: …first Internet governance session of a series of governance sessions that we will be having during this meeting. You all know that Internet governance is a very important topic. It's on the top of everyone's minds. The first session will mostly be I guess what you could call an informational session. We have a series of presentations introducing you to the current landscape.

Our first presenter is Desiree who will introduce us to the current global Internet governance initiatives. Desiree, if you're ready.

DESIREE MILOSHEVIC: So I'm not sure if some slides are ready in the background. Maybe it will take two minutes to have them on, but in the meantime, I'll just say thank you for inviting me here today. Most of you know me as a policy advisor working for Afilas, but I actually have a long history with the ccNSO as well going back to 2000 and earlier, as I'm representative of .gi registry and one of the founding members of the ccNSO back in 2003 when we, as some of you remember, had a small crisis.

I think today the way how to maybe put a slightly broader picture of where we are in the world of Internet governance is to talk about the crisis that is going on today. I would call it a crisis of accountability and the crisis of trust that we have.

For some reason, the slides are not on, but I could be descriptive in terms of what I'm trying to say. When I was invited to say a few words, they said, "Can I say a few words to normal people about what Internet governance is and all the latest developments?" But I think normal

people usually used Internet, and as they get access to the Internet, they don't really care much about Internet governance.

This room here is full of stakeholders that deeply care, and one of the most engaged stakeholders in the Internet governance fora. So as such, it would be very hard to tell you what you don't already know. But I think it's important, as they say, that repetition is the mother of all studying to remind ourselves of some of the paradigm shifts that has taken place in the Internet governance politics and the conversations. Obviously one cannot foresee the risks that are in front of us, and the risk for the Internet, the risk for the technical community, the risks that are in front of us as a society and also the technical community and your part of it running the important parts of the Internet.

So last year I think with the Snowden revelations it became obvious that some of the core principles of the Internet, such as trust, have been undermined, and therefore there are different notions in trying to address the trust that has been derailed Internet as well.

What can we do as a community in order to fix that? Where are we going? What are the obstacles and all of the latest journeys and meetings that we have?

If we try to ask ourselves, did anyone break the Internet? No, the Internet has not been broken. It still runs. But the trust has been derailed, and the NSA has scanned the Internet, so the Internet has been scanned or eaten.

We cannot just speak about one particular player, the NSA. There are many others – GCHQ as well. but we also do not know what other

countries are doing, the extent of mass surveillance that is taking place on the Internet, that is undermining the trust of Internet users and that has huge repercussions on the technical community. So it's not really surprising that a technical community has organized themselves last year with the Montevideo statement and try to address some of the issues.

Following that statement in the IGF we had other events like the NETmundial. Are the slides going to show up at some point or not? Okay, fine.

So what we have is that we need to address this issue in a very coordinated effort. We need to look at how to fix that part of major core Internet principles that is trust in addition to openness and transparency and accountability, and all of these actually leads to innovation that is critical to the further economic development of our societies and the healthy functioning of the system. So I was going to not dwell too much upon – I'm going to move over there. So that is something I already mentioned, that it's been scanned.

Further on, as I said, we're not going to dwell too much because there will be a lot of sessions talking about the IANA transition and panels as well as the NETmundial meeting that took place in April this year, the first so-called multi-stakeholder event that produced a paper, a point of reference that we have as an Internet community that is not a UN document, that is not a document within [inaudible] in any inter-governmental organization, but it is a document that has been produced with a set of [cores] and principles, and some of the resolved issues.

But further on, I think what I'd really like to set the stage here before you go into the detailed is to set a stage about what is required to rebuild this digital trust worthiness among actors and institutions and processes that we all participate in. We will be able to answer these challenges that are in front of us with revelations that are so dooming.

So in order to harken back in time and find out even what Larry Lessig said, that the code is politics but everything around it – the architecture – is the politics. So to put it in a more descriptive picture, I think the Internet geeks and people who have developed the initial OSI stack did really well with 127 on this slide.

So what we need to ensure is that level 8 and 9 does not ruin that for the rest of us. We talk a little bit about the NETMundal. But even before that with the wake of WCIT and we had many sessions here at the ccNSO explaining what really happened there.

I think it's important to say that what is transparent, that it's no longer fine that one country has too much power, and that one country currently is the U.S., although some of the core principles of the Internet actually align with some of their constitutional values, such as freedom of expression.

And what we are seeing here on this picture, I don't know if anybody knows where this is from. Has anyone seen maybe Glenn Greenwald's book "No Place to Hide"? This photo here is actually the NSA's offices taking away a CISCO router from the transport where it's being transported to and using the [fan] to actually take over the sellotape before the spine device could be inserted into the device and then sent back of unnoticed.

I think it's important to say it's just not only, as I said, the NSA that is doing that. So we have a role, as all stakeholders, to try and address these issues and it's not going to be easy at all in rebuilding this trust. It's not unusual that one of the major themes this September during the IGF will be trust and rebuild of digital trust.

I think of this photo here is very descriptive of also what's going on in the world of Internet governance. We have [inaudible] as a representative previous of the ITU, the Intergovernmental Organization, and Dilma. And we have Fadi here who is obviously a character portraying the successful multi-stakeholder organization that we participate in at ICANN.

It is interesting that accountability of ICANN has been brought up and questioned again. This last morning we had a French speaker at the opening session who talked intensely about reform that may actually need to take place within ICANN. I think we have all seriously taken some notes of what the France spokesperson talked about.

It just sounds like a reason to really address, go back to the working session and see how we can build in a view of all recent events how we can make ICANN stronger and who is ICANN going to be accountable to, because at the moment it seems like it's a hanging question.

So I mentioned some of the risks. I think the WSIS+10 was another process that we heard about on Saturday from Nigel Hickson. It's actually reviewing the Tunis Agenda, a very important document that talks about multi-stakeholderism, and for the first time tries to define the different roles that different stakeholders have.

However, it's not conclusive because we know that even such process being in inter-governmental process when some of the stakeholders do participate, will still be decided only in the UN GA in New York.

So kind of trying to think of where we come from and all the tenants and principles of the Internet that you as custodians of networks and national sovereign networks really adhere to the transparency and the innovation that is necessary in order to further develop the Internet.

I think we are seeing for the first time in history a schism between the industry and the governments as well. And this is something that we haven't actually ever had before. We see the Facebooks, the YouTubes, the Googles actively and openly speaking against the mass surveillance. Actually, they have formed a coalition on June the 5th – "Reset the Internet."

What are going to be the important steps of how we're going to take back the Internet that has been scanned, that has been swallowed? How we can actually make it more costly for some of the activities that states are doing to be contained? What are going to be some of the things?

It is nevertheless obvious that the bits of permission-less innovation is a threat, not the architecture. When I talk about the permission-less innovation, all I think is we always use the example of World Wide Web, that the network has to be neutral, so any developer working in his bedroom can actually develop a program that will neutrally run on the TCPIP network.

With the recent debates at NETmundial about net neutrality that have not been resolved, we also see a threat that there is a possibility that many things are at risk, not just media and pluralism, but also the innovation which is the key.

We are really not facing just the multi-stakeholder processes, which are a threat. We talk about it and everyone is sort of sick of pronouncing this long word. But what it really means is that these governance institutions in ICANN that we've been working within are also a threat.

It's all a very complex issue, and maybe that's the problem why – one of the reasons why normal users that just to the Internet and don't want to get involved with a complexity of issues. But I think it's also our role to engage all and make a further awareness within our community of what's going on and what are the necessary steps that we all need to take in order to rebuild some of the trust.

So I think these are some of the reminders. I think for most of the people, the Internet still becomes and it stays the most important thing. But what we are actually seeing is not just the censorship from the sates. We're actually seeing on a societal level. Are we seeing a self-censorship, I think, which is the worst-case scenario because it will prohibit us from any kind of open conversation, intellectual stimulation and eventually progress.

So what we are facing is a risk of the Internet not being further developed and being frozen and the technology being frozen, and in order to address that, I think we have to create this open – as [inaudible] says, open and inclusive space for all stakeholders to participate in this process and to be very compliant with the human

rights and digital liberties. We also have to really rethink about the role of law.

I witness a lot of conversations in the Internet governance sphere where people do not understand even the difference between globalization and internationalization and we keep forgetting that the real risks of separating the Internet and some of the repercussions that are coming from all these recent events could be witnessing further separate state nets, and forgetting about the globalness of the Internet and the real value, which is much different than internationalization and making any institution an international institution.

So I think it will be worth maybe studying a little bit further and paying more attention about [inaudible] and finding some useful kind of references in other spheres as well that we can look at.

But all in all, I think it's about preserving the core Internet values, and it is about one of the core Internet values was the trust and the trust that is being built in this multi-stakeholder process, because we all participate in the policy making development processes. And by doing that and engaging at all stages of discussion, we further built this trust and now it's really important that we get a balanced – to build more balance between how decisions are being made to really make a huge effort between civil society, between private sector and the states how the Internet is governed. Otherwise the future does not look very bright. Businesses will be required more licenses in the area of DNS. It may look like China. Some sites may resolve. Some sites may not resolve.

Lastly, there is, on a geo-political level, I think we are also witnessing that some swinging countries are waking up to the idea of a democratic way of some of these values. They're actually entrenched in the Internet values as well and they're trying to find a way while some of the authoritarian regimes are obviously staying very firm to their values. So it's going to be a challenging time ahead of us to bring that balance back and to rebuild trust among all of us.

With that, I will close. Thank you for inviting me. If there are any questions, I'll take them.

YOUNG-EUM LEE: Thank you, Desiree for a fascinating and a very enlightening overview of the landscape. I think it basically brought us back, made us take a step back and look at what the core value of all of this is and the permission-less development is a concept that I think we should all be aware of. That concept made us aware that Internet governance is much more than just the IANA transition. Thank you very much.

Speaking of governments, I think we can move on to our second presentation by Allan, A Primer on ccTLDs, on Internet Governance, and the ITU. Unless anyone has urgent comments, I think we should take comments at the end of all presentations. And since we are pressed for time, I'm sure the rest of the presenters will be mindful of the time limit. We have until 12:00. Thank you. Allan?

ALLAN MACGILLIVRAY: Thank you, Young-Eum. Actually, thank you, Desiree. I don't think you said IANA transition only maybe once in the whole time. That's a bit

what I want to talk about. I think two years ago all of the talk was the WCIT and now we as a community have moved on to IANA transition. And really what I want to talk a bit about is the fact that the issues with respect to the ITU, the debate over multi-lateralism versus multi-stakeholderism has not gone away. It's still very much alive. There are meetings happening this year. I think you were alluding to a number of them, and I hope we can talk about the ITU Plenipotentiary Conference in South Korea in October.

So what you see up on the screen there, actually, I think it's a misrepresentation, because really, this is a trailer for the movie. You're not actually going to see the movie. I'm going to talk about a paper that CIRA, .ca, partnered with CENTR and LACTLD which is a primer for the ccTLD community on the ITU and also with respect to Internet governance. How do I switch here, Kristine?

So what we did is we commissioned a paper that comes in two parts. The second part actually is just a straightforward background briefing on the ITU. It's quite short. It's only about six or seven pages. It's written by a fellow by the name of Don MacLean. He's a fellow Canadian, so he's a good fellow, who once upon a time worked at the ITU but long enough ago that he's trustworthy.

So that's the first piece. It's available in English. It's also available in French, especially for [inaudible]. I knew that he would like that. And [Carolina] has had it translated into Spanish, so it's there as well. Actually, we're getting good traction. Peter can speak to this after. I think it's a very good piece.

The second piece, which is really what it tries to do is to build on that background on the ITU to explain why the ccTLD community should pay attention to what the ITU does, because it remains an issue. So there are meetings this year. We talked about the WSIS+10. There's just a lot of misunderstanding. I think Desiree spoke to this as well. People don't understand terms.

I can speak to as a former government official who my office was three doors down from Heather Black's at Industry Canada, and until I joined CIRA I had never heard the work multi-stakeholderism. So I can assure you that there is a dearth of information in many countries amongst the community that go to the ITU meetings, and they would really benefit understanding what we do and how we do it because it's very foreign to them.

So what we do in the paper is explain why you as a ccTLD community should get engaged. I can assure you that there's a demand amongst national governments for this kind of information, and I very much encourage you to do that. If anyone's in the least way reticent of how to do that, come and see me and I can help you write something. It's a very straightforward process.

That's really what my message is today. I should mention that the second paper was written by Samantha Dickinson from Australia. I'm sorry. She did an excellent job. I can compliment both pieces, because I didn't write them. I have some copies in English, French, and Spanish. Both papers are up here, if anyone wants to just come and pick up a copy. They're also available on the CIRA, CENTR, and LACTLD websites. That's it.

YOUNG-EUM LEE: Thank you, Allan. Now we move on to China and what China has been doing with regards to trying to maintain the sustainability of the Internet. And we have Xiantag Sun from .cn. Thank you.

XIANTAG SUN: Hello, everyone. My name is Xiantag Sun from .cn, China. Today I would like to talk a little bit about the Internet Governance for Sustainable Development.

As everyone knows, China is now is one of the biggest developing countries. Now, we are serving as the national ccTLD serving. Now we are serving one quarter of Internet users of the world. We are very proud of it. Today I'm going to share a little bit about how CNNIC as a national ccTLD, how we perform and what we do in the Chinese Internet I call system.

I know the Internet governance issue now is so much popular. Of course people want to listen how the Internet governance situation in China, I think that's our minister [inaudible] job and [inaudible] stay in this position to talk about how CNNIC as a ccTLD registry, what we do in China and how we serve the people.

Before I start on my presentation, I would like to share one thing. China is one of the biggest developing country, so when we talk about the Internet governance issues there is a scenario. The scenario is we are developing. It's a dynamic process. So that will explain a lot of things. That would explain what we do.

The numbers. Here is a number again. You can read and hear a lot of presentations from the Chinese side. At the moment, for example, we have 600 million Internet users [inaudible] mobile phone users, etc.

When we talk about the numbers again and again, actually the purpose of this is not to show off how many users we have. It's a reminder – for me at least – it's a reminder to remind when we talk about Internet governance, especially for a developing country, especially for China.

The reasons why? I think the key point is when we talk about Internet governance, the final goal is how to serve the people better. And when we define the principles, when we talk making plans, we always – sometimes we forget. At least from my situation, sometimes we always forget and we focus too much on the principles. We focus a lot of attention on the solutions themselves. We forgot who and why we serve for.

These are the seven principles from our Minister of China, Cyberspace Affair Administration. The seven principles, my personal understanding of the principles is Internet governance should serve the people and should serve the peace and is for the development. I think I have a deep understanding of this, because of why? Because China is one of the biggest developing country. We, in the past 10 or 20 years, CCNIC as an example, we start from scratch. And 20 years ago, we even don't know how to set up a DNS server, but now we are one of the biggest registries in the world and now we [recover from 300] .cn users three years ago. Now we have [inaudible] again.

So we communicate and we learn. And all those things is in the process of developing. I hope the experience from China and from CNNIC could

be shared and also useful to other developing countries, and that would solve a lot of issues and improve the conversation and collaboration between the developing and the developed.

This is what we do. This is a very draft scratch picture of how the Chinese Internet ecosystem. You can see the end user government research CNNIC [inaudible] how CCNIC is performed. I think one of the core values of the CNNIC developing strategy is everything, every plan, and every single cooperation strategy is for development and is for cooperation.

So from this page, we can see CNNIC is a ccTLD registry. So [inaudible] people think a ccTLD registry, what he should do is to manage .cn, but actually in our ecosystem what we do is already more than a ccTLD.

We are in the [inaudible] developing process, [inaudible] the Internet has a very fast development in China. The history and also the situation gave CNNIC more functions to form, and also after years after years, people have more expectation of CNNIC.

So this is our goals in Chinese [I call] Internet governance ecosystem. First, of course we are running .cn as a registry. But also, because the domain name is the basic fundamental resource of the Internet, when people use the Internet, it's the first thing they visit. Now we are a platform of cooperation in China, [business], government, research, international organizations, domain industries, they all come to CNNIC as a platform to communicate. So this is more than a traditional TLD registry.

Also, we are a link from China to the world. I mean, without the help of the world, I can't imagine we can improve our technology and the techniques. Also we join a lot of ISTAR organizations.

So when we grow bigger and faster and faster, some people have more expectations. This is how people think, how CNNIC should perform in the Chinese Internet governance ecosystem.

So first of all .cn represents the country and also the language, Chinese. Also, this is a kind of public trust. When people choose .cn, they choose a national trust credibility, and also as a fundamental resource. This is how the industry, government, research, organizations all come to us as a platform.

Also, we do a lot of nonprofit things and we keep doing the research. We have more than a 100-people research team and capacity building [passes] the bridge and solve problems and also international cooperations.

So those kind of things is already beyond the scope as our traditional ccTLD, and this is how we perform. This is our role in the Chinese Internet governance.

So capacity building, a lot of people think capacity building is to improve the capacity and to solve the digital gap only. But for us, from what we have done before, in terms of the Internet governance, we found capacity building is crucial to solve the problem. One, there's no current solutions. When we talk of governance issues, there are reasons behind my opinions. Number one is problem and the questions always comes

because the gap of capabilities, because of the gap between the developing and the developed.

So when [accountability] because [inaudible] and become the gap, when the gap of interest become [inaudible], there is much easier when people get consensus, especially when we talk about Internet governance issues.

So in terms of that, we will keep doing the capacity building. And also this is one of the biggest directions CNNIC is going to do, especially when we talk about the Internet governance. We have some [inaudible] resource, so we welcome all the registries no matter in Asia or other continents. We're always here and happy, friendly, open and we welcome all the friends join us. Thank you.

YOUNG-EUM LEE: Thank you, Xiantag, and thank you for the very informative presentation on the many, many activities of CNNIC. Next, we move on to another more specific area, The Influence of the Great Trade Agreements on Internet Governance Policies in Latin America. We have Celia to introduce us to that topic. Celia?

CELIA LERMAN FRIENDMAN: Hi, thank you, Young-Eum. I'm Celia Lerman. I'm a NomCom representative to the ccNSO Council. I'm a representative of the [inaudible]. I'm a member of the Business Constituency and a professor of the University Torcuato Di Tella. It's in this character that I'm going to talk about today when the presentation is going up about research that

we're doing together with the University of Pennsylvania in the United States at the Internet Policy Observatory that they have.

It's interesting because this is a topic that really touches on the importance of multi-stakeholder participation for implementation of local policies at the national level. So we're going to talk about free trade agreements in Latin America and the Caribbean.

And this really touches on a topic that we have been discussing at the ccNSO. In the Buenos Aires meeting, this topic was discussed was "Update on the Leaked Trans-Pacific Partnership Agreement Document."

Yesterday we had a discussion at LAC SPACE and we had the participation of Margarita from NIC Chile, because it's really interesting to have the cc's perspective on this topic.

So what is it that we talk about? Well, this trade agreement – there had been, since 2003, trade agreements between different countries – the U.S., a few different countries in Latin America. It's 11 countries. Bilateral treaties and regional treaties. Even though they do not mention the Internet, they do have an interesting impact on different topics such as domain name, dispute resolution, ISP liability, e-commerce, data protection, telecommunication. They also have some disclaimers on the flexibility to apply [these classes].

Some of these treaties, like I said some are regional, [inaudible], and some are bilateral. The first one was the one with Chile, and then they had [inaudible] with Panama, Colombia and Peru. And now I put Mexico

because it's in the process of negotiating in the Trans-Pacific negotiations.

So these treaties can have a fundamental impact on the Internet policy in countries because they establish local policies that can sometimes be not taken to account the traditions and the legal cultures of the countries.

And that raises into problems of implementation of these treaties, and also raises on the importance of having really a multi-stakeholder discussion of this, which is sometimes hard because these negotiations are usually secret.

The treaties are being negotiated now, for example, the TPP, is usually known through Wiki Leaks. That's what we know of them. They come leaked in the end, but having a more open discussion really helps to have these treaties well-implemented.

Let's take an example that really touches on the ccTLDs operations. For example, on dispute resolution, these treaties establish – I'm saying each treaty is different. Of course each treaty has its particularities. But in general, they replicate [inaudible] with minimal differences.

So the original ones say each country should have a dispute resolution procedure to protect trademark, to avoid trademark cyber piracy based on the principles of the UDRP.

This implementation has been, for some countries, in Latin-America has been challenging because they really didn't have any dispute resolution system and they had to comply. These treaties were negotiated by the government, and then the ccs had to implement it sometimes in a rush.

Now the questions are evolving. So for countries that did not have any original – any trade agreements in effect yet, they are at the [inaudible] negotiating them to be more broad to really accommodate and have more flexibility, not only UDRP, not only in trademarks but also geographical indications and trade names to accommodate the systems that they already have in place.

And not the UDRP only, but also systems that can be equivalent and also that let you go afterwards to court systems in order to respect the national law.

So what we have been doing in the research is gathering together the experiences of different countries that I want to share with you today. In some countries – and I think very much the ccs that have been helping us their experiences, but what we've seen is that, for example, in countries such as Guatemala or Peru, they did have a system in effect at the time of committing to these trade agreements. The impact was more [moderate].

But countries like Costa Rica, the problem was that when they [inaudible] to the treaty, they had a short span to adopt the dispute resolution system, they didn't have the local expertise to adopt a local system to do that in such a rush or in the timeframe that they were given, so what happened is they ended up sending their disputes to WIPO, and WIPO was very generous with them and they worked it out.

The problem was that when they sent it to WIPO, they had no disputes for a couple of years at all because people even – the experience that they shared with us was people even preferred to send their disputes to private arbitration in Mexico, because really they were not familiar with

sending local disputes to Geneva. Imagine Costa Rica, Geneva. It's something that's a different language, different culture, far away – even though WIPO is international.

So what they ended up doing last year – or 2012, sorry – they implemented a multi-stakeholder [consultive] council where one of the working groups was, well, how do we implement this at the national level? And they started to accredited and national – the local bar association is now able to, besides WIPO, resolve these disputes.

This is one example. For example, in [Salvador], instead of sending the disputes to WIPO, what they decided was to implement it through the National Chamber of Commerce, but now they are not having any cases and one can wonder, well, is this a problem that people see as very far from them?

And the last countries where it didn't have the impact that they already had a system in mind, well, [do these] treaties take the flexibility that they need out from their implementation.

To conclude, I want to give some remarks. I think the FTAs are really sometimes a great opportunity for countries that, in Latin America where sometimes the Internet policy discussions are not in place, they are really an interesting opportunity to consider these topics and implement sometimes policies that otherwise would have not been implemented.

But at the same time, it could be a challenge for local implementation, because if it, for instance, takes the flexibility [inaudible] country needs

to implement – for example, the other operation that we haven't talked about is WHOIS provisions in these treaties.

Now that the WHOIS system is being reconsidered and they are going to be global standards for WHOIS, what happens with these treaties is they are already fixed a system for registrants. It's okay. It's at the ccTLD level, but it could still accommodate more flexibility.

The role of multi-stakeholderism is now registries are negotiated by governments, and now some countries are incorporating other stakeholders in the discussion besides their local diplomats. And this is very important to be able to implement these treaties really in an effective way.

And our point is the importance of flexible provisions that can contemplate national law. Local disputes are not going to be sent so far away. For example, so can we really give them the time to implement a national – or even regional – dispute resolution systems?

And another fact that is key is sharing experiences among countries. For example, the experience of Chile was very valuable to other countries since they had implemented their own dispute resolution system, and that led the way for other countries. Thank you very much.

YOUNG-EUM LEE: Thank you, Celia. We have about ten minutes. Any questions for the presenters or questions or comments on the topic of it governance for our presenters? Microphones will be brought to you by Gabby.

[CAROLINE]: Thank you. This is a question/comment for Allan. Allan, are you aware of ccTLDs that will be participating at the plenipotentiary in October in Korea?

ALLAN MACGILLIVRAY: Actually, [Carolina], I'm not aware of that. It's something that we and CIRA have discussed participating. I don't think we've made a final decision. Unfortunately, the first engagement with our government was last Friday. They held a meeting. We were invited. It's just that we were in London. Certainly it's something that we're actively considering.

YOUNG-EUM LEE: If I may also add to that, since ITU is only open to its members and official representatives of government, I think in order to participate in the ITU, you need to establish a very friendly relationship with your government in order for you to be able to attend.

ALLAN MACGILLIVRAY: Actually, I'd just like to draw a thread between what Celia said and I did, which is although Canada's not a Latin-American country, we are engaged as one of the partners in the Trans-Pacific Partnership. Even though I think we enjoy a close relationship – rather an appropriate relationship with our government; I wouldn't say close – we, like a lot of people, found out about some of the text on URP from Wiki Leaks.

But we were able to engage them and to educate them, and we think that we were able to get some of the language tweaked to make it conform to the particular practice we have in Canada. And I think it just

goes to the general point of engaging your government, because they will do things that will have an impact on you and sometimes they don't even know you're out there.

And I can say, speaking from experience, governments can be quite arrogant because they think they're at the top of the pyramid so they don't have to engage.

Unfortunately, sometimes the initiative has to come from you as a community. So it's something I would encourage you to do, because things are going to happen that will have a direct impact on you and I think you may have to take the first step.

[YOUNG-EUM LEE]: Again, I think NETmundial was an event that allowed such an interaction between the ccs and the government. I guess the world is slowly coming together, even among the respective national ccs and the governments. Yes?

[CAROLINA]: But again, echoing Allan's recommendations I would strongly like to urge all the ccs to engage actively with your government representatives of the ITU, because they will be talking about Internet governance issues.

UNIDENTIFIED MALE: Yes. My question/comment is about [future government's] position. Is it desirable that ccTLDs share a uniform, almost identical, regulation? Because if it [inaudible] specific with a WHOIS clause and the dispute

resolution, is it good that they are all the same or we want diversity, we want to let ccTLDs to really embrace the local needs or [want] uniformity and predictability to improve the [immersion] of ccTLDs in the world.

CELIA LERMAN FRIEDMAN: I'll go first, and then [inaudible] continue. I think it's interesting what Allan was suggesting. I think it's interesting that if countries get engaged even if there is a common text, I think if the text is flexible enough, there could be appropriate national implementations that take into account these local traditions and the local culture.

[DESIREE MILOSHEVIC]: So I guess the keyword is flexible.

XIANTAG SUN: Hello. So from my point of view I do think there are common things. I mean, [inaudible] make among the ccs, because those are the things, those are the [inaudible] points should be the basis of a collaboration, especially for the breach between the developings and also the developed.

But at the same time, I would like to point out different countries have different scenarios, especially for developing countries. For example, we use chopsticks, but we are not against a fork and knives. It doesn't mean we don't know how to enjoy the food. There are a lot of things – [inaudible] we can do the capacity building together and there's a lot of things in common we can share.

So in this point, in terms of your question, I do believe the purpose that we are here is to find the [commons] and reserve the difference and find solutions.

YOUNG-EUM LEE: Margarita?

MARGARITA VALDES: Something interesting in the case of Chile facing the TPP agreement. Having before a TLC agreement with U.S. that the negotiators are very strong in the position that the TLC was before, so we can't move more than in the TPP text. We will not move in any place different at the TLC, because in some parts the TPP is more exigent or more aggressive – I don't know the word – in the text. But we feel very comfortable with the TLC that we already have.

So probably one recommendation, if our colleagues could approach to their governments, try to analyze what is the scenario – [inaudible] scenario – in terms of the trade agreements, and then you can probably see better the written text in order to not permit more than that.

YOUNG-EUM LEE: Okay, thank you. One last question, if there is one. Okay. We seem to have run out of questions. This brings us to the close of our session at exactly 12:00. I now pass the session over to the second topic on Internet governance.

KEITH DAVIDSON: Okay. Could I ask everybody to take their seats and we'll resume the ccNSO members meeting? [Kristina], could I ask, is anybody online and participating? Okay, thank you. Could everybody take their seats, please? Thank you.

Welcome to this afternoon's first session. It's a one-hour panel discussion. The title of the session is "Perspectives on ICANN's Accountability Process" and the purpose is to explore some of the ccTLDs' perspectives on the process to enhance ICANN's accountability. And within that, this explores the scope and the process and the potential relationship with other discussions and processes such as NETmundial, the ATRT-2 and the NTIA stewardship transition process.

And for those who don't know me, I guess I should introduce myself. My name is Keith Davidson. I'm the vice chair of the ccNSO Council and from .nz.

Could I firstly walk us down the group on stage today, and could you all introduce yourself very briefly your name and affiliation and what interests you're representing today. Firstly, Theresa.

THERESA SWINEHART: We had the ALAC meeting yesterday and there was a different approach to buttons. It's a long story. Theresa Swinehart, senior advisor to the president on strategy. I work for ICANN, and therefore I work for you. So that's that.

LISE FUHR: Lisa Fuhr, I come from the Danish registry, .dk, but I was also a member of the ATRT-2 group.

AXEL PAWLIK: Axel Pawlik, managing director of the RIPE NCC and I think representing the interest of the [inaudible] community.

CHUCK GOMES: Chuck Gomes with VeriSign and the gTLD Registry Stakeholder Group.

KATHY BROWN: Hello. I'm Kathy Brown and I'm with ISOC, the Internet Society, and I represent the interest of the Internet.

BECKY BURR: Becky Burr, .us.

MATHIEU WEILL: Mathieu Weill, .fr.

KEITH DAVIDSON: Thank you, all. Becky and Mathieu are here to start to pose some initial questions to the panel when we get to that point. Then as we move through this hour, the last 15 minutes we hope to dedicate to a public Q&A. So be working on your questions. What I'd like us to do is all have brief questions and as briefer responses as we can. So if we can contain ourselves [inaudible] rather than posturing or trivializing any issues and

stay on topic and really focused, because I think this is a topic that could last for several hours rather than the brief time we have.

But firstly, we have an introduction from Theresa to explain the process and scope from ICANN's perspective. So bear with us. I understand you have some slides, but you have a hard ten minutes.

THERESA SWINEHART: You keep time on the watch and I'll talk.

KEITH DAVIDSON: Okay. So I'll hand it over to Theresa for the introduction, and then I assume it will be okay with you if you remain as one of the panelists.

THERESA SWINEHART: Happy to.

KEITH DAVIDSON: Thank you. Okay, all yours, Theresa.

THERESA SWINEHART: Okay. So very quickly, first thanks for the change in the picture. It looks less conspiratorial with the sunglasses. That was very lovely. And just a second, I think at some point we should form working groups on how to find rooms, because this one is quite confusing. Anyway, on to the more important things.

So to give a quick update on the session here, I was also asked this morning whether I could touch very briefly on where we were with the

NTIA IANA stewardship process. I think everybody's aware, but I'll run through that quite quickly. So next slide, please.

So on the sixth of June, the process was posted and that was based on a tremendous community input, including from the ccNSO and from several of the regional organizations. So thank you very much, first of all, for the input and for the effort that went into that. It was very important. And I hope that everybody feels that a lot of it has been captured. As you know, we receive quite a bit, so it was a balancing of the various views that were provided.

There's a quick listing of some of the key changes that were made based on the community input and the fundamental part is also that the Coordination Group names are to be submitted by the second of July, and the Coordination Group itself has responsibility to identify and work on the charter and working methodologies how it will be conducting its work itself. So that will be the responsibility of the Coordination Group.

There was quite a bit of input on that topic, and hopefully the Coordination Group will take a look at that. Some very good input also from the ccNSO and regional cc organizations. Next slide, please.

This is again just an overview. The slides will be made available so you can have those. Next one.

As I said, call for names on the second of July. There's a face-to-face meeting in mid-July to begin the initial work of the Coordination Group. We've already received names coming in, so we look forward to be receiving more of those. Next slide.

This is the composition that's available online. As you can see, for the ccNSO and the ccTLD community, there's a number to try to address some feedback that we had gotten in that process as it also occurred with several of the other stakeholder groups. The total right now of the group is 27 representing 13 different communities. Next slide, please.

So let me get to the enhancing ICANN accountability. This is, as you're aware, a separate but very inter-dependent community process. I want to state up front very clearly that the document that is posted that has been put out for community input is a proposal. It's a draft. It's for community input. The comment period is not over. And so that is on the 27th of June. We're receiving a tremendous amount of comments, and once those are all in, one can take a look at, with all the comments provided, what is the right next step and approach? So I just want to be quite clear on that. I know that the ccNSO has already provided some comments and those are very, very useful and we'll look forward to reading those obviously with everything else.

The proposal, as you're aware, has a proposed scope to look at the issue around ICANN accountability in the context of the changing historical relationship with the U.S. administration in light of the U.S. administration being willing to move its stewardship role to the global community.

There is a view and there is a perceived view that there is a backstop [role] for the U.S. that it has in the context of ICANN's broader accountability, and so that's an issue that we want to be taking a look at, in the context also of existing accountability mechanisms, what could be strengthened, where are the gaps and how does that get addressed?

Certainly I know from discussions that there has been discussion about what is the individual accountability aspect of a cc in relation to the IANA function? That is obviously a topic that's very important. This is looking at the broader topic of ICANN accountability in the context of its changing relationship the U.S.

The deadline for public comments and reply periods was extended based on several requests that were received and that was responded to. And the current deadline is the 27th of June. Next slide, please.

Again, I said that there's an inventory listing. It's not exhaustive in any way. These are some of the categories. You'll see also in the hallways some whiteboards where one has the opportunity to provide feedback on those categories and on topics around this entire process. So really a lot of outreach is being done on this along with obviously the posted document. I hope you're keeping time. Next slide, please. Okay.

Call for input. Obviously on this the proposal output would look to identify the key elements for strengthening ICANN's accountability, again in the context of the historical change in relationship.

Prioritizing those elements for development and/or refinement. There's been a lot of different themes discussed in this area. It would be important to also look at how to prioritize those for development.

And then setting forth a timeline and mechanism for the implementation and improvements of anything identified. Some things may take quite a bit of time. Some things may be shorter based on how they're being prioritized. Again, also being reflective and respective of the workload for the community overall. Next slide.

Here you'll have a listing, and this is obviously in the document, on what the proposal is. The concept of a working group is something that we've heard so much about in the community, including with the ideas of the cross-community working groups and it was certainly a theme that came up in the discussions at the Singapore meeting around accountability. Hence, that proposed direction was taken. But again, this document is still out for public comment. Next slide, please.

These are some subject matter areas in the context of accountability overall, where if the working group model is pursued, expertise around these specific areas would be needed and called for. Next slide. There is no next slide? Okay, that's it. Then I am done, and I look forward to the conversation.

KEITH DAVIDSON: Excellent. Thanks, Theresa, and spot on time. Over to our interviewers. Do you have some questions aligned?

BECKY BURR: We're going to do a famous [inaudible] of walking around people, because we decided it would be more exciting, although watching me walk could be more painful than anything else.

So we have people who have been around this community for a really long time. Chuck, I am looking at you. And some who are more newer to the environment. Kathy, this is like trial by fire.

I think that if we could first start out with you, just tell us a little bit about what the ATRT-2 findings were and how you think that plays out

in this. As we are going forward, thinking about accountability, what we ought to play particular attention to from the ATRT-2 perspective.

LISE FUHR: Well, the ATRT-2 group, we're picking up on the first report from the beginning, and the first report actually made – there was a Berkman report on accountability as such. What we tried to look at was accountability in the DNA. Is it really embedded in how ICANN works? How can we measure it?

I think how to measure accountability is a different task, and that was actually one of our most important findings. We found that there were no measurements of accountability and we should try to find a way to benchmark accountability and to see can you measure it, and if you can, you should have some metrics for doing this.

I think that's another thing going on. It's important that accountability is very visible. So if you're accountable but not showing it, then it's not going to work. Then you'll lose the trust.

MATHIEU WEILL: Thanks, Lise. I think the value of this panel is to share different perspectives on what's expected by accountability, which is a weasel word right now within ICANN. So maybe starting with Axel, [inaudible] community, obviously. And if you look at ICANN and its accountability, could you explain us in very concrete terms what's at stake for you and what the issue is that you want to improve or maintain in the discussions that are to come?

AXEL PAWLIK: Sure. As you can probably see from the relative non-prominence of the RIRs in the big ICANN sphere, our interaction with ICANN is really focused on getting numbers from IANA. That's our main interest here. I wouldn't say that's at stake. I think we are very happy with the IANA workings for a very long time, so that's looking good.

I think the key feature here is that the operations of IANA and the policy-making process are very nicely and clearly distinct in an organization. The ASO MoU has established the policy-development process for allocation of numbers to the RIRs. That's a global numbering policy. That's again very precisely focused on just that.

The operational frequency that we interact with with IANA overall, all of the RIRs is really, really, really small. A couple of times per year. It used to be with IPv4. With IPv6 I think it's a little bit less even. So there is not that much of an impact.

In terms of what could be improved, I think giving this set up, IANA oversight in that sense, the allocation of numbers is done by the RIRs. I think IANA is IANA/ICANN in that sense are accountable to the RIRs for their particular function, and [inaudible] to the RIR members and by the communities.

I think in terms of improvement, there isn't that much to be done for that one apart from improving the documentation or making it clear or making it more explicit even. I can assure you that the RIR is at this very moment working on a document that lays it out very clearly what [our

corporate] governance is and how that relates to the IANA function for us.

MATHIEU WEILL: So very operational focused.

BECKY BURR: Why don't we ask Chuck the same question?

MATHIEU WELL: Yeah.

CHUCK GOMES: Thank you. Well, the gTLD registries are very similar to the ccTLD registries in terms of a direct impact we have in terms of the IANA functions. We obviously depend on gTLD top-level domains being entered into the root, just like you do. Updates to contact information and so forth.

So the security and stability of the IANA functions, the reliability of that, the timely responses is very important to us and we are obviously one of the directly-impacted parties with regard to this transition.

BECKY BURR: But what about accountability? So we've heard from the RIRs that things are working pretty smoothly. They've got some processes. Documentation could be a little bit better. From the names perspective, the world is a little more complicated, isn't it?

CHUCK GOMES: Yes, it is. And especially for gTLDs, and this is an area where we differ significantly from the ccTLDs, because we are required by our contracts with ICANN to implement policies that are developed in a bottom-up multi-stakeholder model and are considered consensus policies. So we have that added implication.

So the accountability of ICANN is possibly even more important to us because it has huge impacts in terms of our business models and our ability to successfully operate in a very competitive environment.

BECKY BURR: So, Kathy. Kathy is actually not really newcomer to this, because she and I were colleagues at NTIA many years ago. Since you've come to ISOC and since you've been immersed in this, what are your observations about accountability at ICANN and where would you like to see the focus of this process go?

KATHY BROWN: Thanks, Becky. So I'd like to try to parse a couple of different layers. One is ISOC is a home of the IETF and I'm very careful never to speak for the IETF, but I would say to you that just as the RIRs have a notion that the technical aspect of what goes on inside IANA is well-oiled, is the same with protocol parameters.

Those standards are set by the IETF. They're reviewed if necessary by the IAB and they're published by IANA. So it is the publication of those

protocols that is the function of IANA, and that works fairly well. There's not really an issue here. It's been working well all along.

The publication is the only thing that is happening within the ICANN structure and that is happening at IANA. And the work of the standard setting is done pursuant to the processes and procedures of the IETF which are well-documented, transparent, and open to the world.

So with respect to that piece of the accountability, we feel that it's covered. What isn't covered is the asterisk to the whole deal that says, "And oh, by the way, this is all under contract with the United States government." And so the question then becomes what replaces that? So it's not really about, in our view, the IANA transition. It's about the transition away from NTIA, what then becomes the interface, what is the mechanism by which this contract, if you will, goes forward.

So that's with respect to the rather narrow technical issue. With respect to the overall issue of accountability, I think that ICANN has wisely said there's a technical piece that has to be looked at, which includes now 27 various different folks that represent various pieces of this, but which, in my view, we ought to keep a close narrow eye on whether the accountability for the technical aspects are covered – so with respect to protocol parameters, with respect to numbers and respect to names.

And that we ought to be fairly, in my view, clear about how to think about that from a technical point of view. The accountability issue then has been put into yet another conversation about the larger issues of ICANN as stewards. And in that area, it seems to me that there are numbers of issues that have been raised that ICANN has said, "We're going to allow the community to engage. We're not going to be in the

middle of it. We're going to hear back from you and we're going to respond." So that is all to come.

What's ISOC's role in there? It is my view – and I'll see my Board later this week – that we ought to let ICANN and the community go ahead and discuss those issues. We had a large conversation with our own members last night about this issue. We're hearing the input and our members are in many places around the community and they ought to be involved somehow in that conversation, and we think that should happen.

For ISOC, the overall stability of the whole of the Internet with the ICANN piece as part of it is something we want to keep our eye on. So as this process goes forward, I think we will stay in a situation we're talking about the security and resiliency, openness, etc., and availability of the Internet to everyone.

MATHIEU WEILL: Thanks, Kathy. I wonder if Chuck – because we're talking about accountability in quite general terms here, and I'm really focusing on the wider accountability process, not the IANA one. And Chuck, you rightly said the [gTLDs] and the registries in the [gTLD] world are in a different position than the ccTLDs. I wonder if you could elaborate on what you expect from the accountability discussions, and especially on what problem is trying to be fixed from a gTLD registry point of view with ICANN's accountability.

I think it's important for this community to have a detailed view, not just a generic description of terms, but what in concrete life of gTLDs should we improve in terms of ICANN accountability?

CHUCK GOMES: Sure. The critical issue I think for gTLD registries is that there be independent accountability, not just internal accountability within ICANN. Some of those mechanisms work very well. In fact, the ATRT, we were very pleased with the work that's been done by both of those teams.

But it's very important to us that there be checks and balances and mechanisms by which the community can challenge decisions made by ICANN if they are not abiding by the multi-stakeholder principles and processes that we've agreed to, so that independent actually beyond what's available now.

In the past we have had NTIA has played that backstop role. They haven't been real active, but it was there. For example, with the renewal of the last IANA contract. It wasn't issued at first, because the response was inadequate. That was just a check there and a means to improve what was needed there. And that is very important to us.

MATHIEU WEILL: Okay. So, independence.

BECKY BURR: Independent review and redress. So, Lise, I wonder if you agree. Chuck is making a distinction between the fact that ICANN has – that the

policy-making role with respect to gTLDs is a little bit broader than it is with respect to the ccTLDs.

There's an, I hear, concern in the ccTLD community as well for the broad accountability issues. So why should the ccs care about this?

CHUCK GOMES: Well, that's better for them to answer than me, but I think with the exception of the contractual terms that bind us to consensus policies, we're impacted the same way. If a country code top-level domain, for some reason – and I can't imagine this because I have great respect for the ICANN Board. But if for some reason there were some political reasons why a particular ccTLD was treated differently, you would be very concerned just like we would if we had an issue with a particular gTLD issue that was inconsistent with the multi-stakeholder positions on that.

BECKY BURR: Lise?

LISE FUHR: Well, even though we're not dependent on ICANN, we're a part of ICANN and I think ICANN is very important for the ccs, meaning that this is a community where we share governments, we share a business, we share ccTLD registries and you have the multi-stakeholder model and that is very important to the ccs, too. If you change that, we'll have the risk of the ccs being under control of the governments.

So the accountability is an important thing, because if you lose that from ICANN, you might lose a multi-stakeholder model.

MATHIEU WEILL: Trying to push it further one step further in the discussion, Axel you mentioned your expectations which are really focused on IANA and you know there are two different tracks and processes – one for IANA and one for the wider accountability. What if those tracks converged? Would you mind, as a member in community, if the accountability for IANA – basically, the way IANA would react – was the same as for domain names [with the] cc or gTLD processes?

Are you ready to participate in this discussion or do you want them to be separated?

AXEL PAWLIKE: No, we are here ready to participate of course. And of course accountability is part of a bigger world we're all living in and we do, of course, see in our day-to-day interactions with governments, regulators and all members throughout our service regions that ICANN isn't always equally popular. Because they are dominated by the U.S., they are owned by the U.S. and they run the Internet, we all know that [inaudible].

So any kind of explicit accountability to somebody else but the U.S. government I think will make things easier also in our dealings with the rest of the world. It's not just the numbers of course. We are part of the ICANN world just as well.

[BECKY BURR]: So I think Lise made a very important point, and that is that what's at stake here is not just what ICANN says to gTLDs or ccTLDs, but the resiliency and the continued viability of the multi-stakeholder model, which I assume is very important to the numbering system, very important to the IETF, very important to the Internet in general. That's a critical issue.

The question is what is it going to take absent the big stick back here that may never be used? What is it going to take to make sure, because we're moving away from that, to make sure that this system continues to be resilient enough to resist being overtaken slowly or quickly by something that is a more top-down more-governmental, more inter-governmental approach. Anybody?

[KATHY BROWN]: So it seems to me that the ideal answer is a system that works efficiently, effectively, fairly and people feel satisfied with the outcome. So if you have an organization that's working well, working efficiently, is seen as fair, is trusted, it ought to work and the world should be happy.

My concern is someone is always unhappy. It doesn't matter how efficient, effective and fair it is, someone is going to say, "But you weren't fair to me."

So the issue becomes, in my mind, how you deal with that. So first, assume you're going to build an effective, fair system. You worked at that for many years. You keep working at that. I think that always can be better and I think most folks find that there's improvements to be

made, but I get the overall sense that we like this. We like it better than the alternative, right? We, the people, run this thing.

The issue becomes when someone things they're aggrieved, then what do you do? Where is the appeal? Where is the backstop? Where is the ability to resolve that?

In my view, as I look at this, it seems to me that it would be good to focus the conversation. How does that work? Where does it work? And in what way and in what aspects are there issues that need to be resolved?

I don't think this is too – it's not a mystery. If you have any sort of body that's making decisions of value – and these are value decisions, both for the customers who come and want the service, but also for the world that have third-party interests out there. Then you have to have some way of dealing with those who end up unhappy. I hope that part of the work stream is to think about that.

BECKY BURR: Anybody else?

[CHUCK GOMES]: Well, I totally agree with Kathy. And that's what I was talking about – the checks and balances and the recourse when it's needed. Hopefully we won't need it much, but it needs to be there when we do and it needs to be something that's supported by the whole community and respected by the whole community, and not just U.S. space like [Axel] said.

I'm encouraged by what I'm seeing in the environment. There are lots of ideas – concrete ideas – that are being discussed in the community, and I think it's going to be a quite interesting exercise for us as a community, not just the coordinating group, but for the community to evaluate do due diligence on these ideas and come up with ideas that all of us can support. And then I think that's going to strengthen ICANN. It'll give ICANN more respect and be good for all of us.

MATHIEU WEILL: Axel, would you like to elaborate on this idea of independent recourse?

AXEL PAWLIK: I absolutely agree. I think this is our organization. We built it together. We need to improve it jointly and be willing to accept the outcome with maybe a rough consensus, but it's out organization and we need to support it. We need to continue to support it. Yes, independent recourse is important. We do have that RIPE and to see as well through [inaudible] very low key, very boring stuff – just numbers, no trademarks, no geographical names, nothing like that.

So it's simmering on a very, very low fire there. But we have that and that is things that are important.

BECKY BURR: Lise, when you talk about this, I want to ask one particular question. We do have some accountability mechanisms out there. They're pretty expensive. And I think it would be useful to talk about how important it

is you think that these independent recourse mechanisms be accessible outside of the multi-million dollar commercial dispute context.

Okay. If you don't want to answer that, you don't have to.

LISE FUHUR: Because I just wanted to get back to the other one, just a short – what I think is very, very important in this whole process is that ICANN in this search for accountability reaches beyond the ICANN community and we need to involve more, because ICANN is of course at the core of the involved parties, but we have a lot out there who needs to be involved. And if we want this to be a long-term solution, I think we need to involve more.

And about importance of very expensive metrics, I don't think they need to be very expensive. I know the ATRT-2 team, that's expensive, but I think both parties learn a lot. The team learned and can spread the word that we're confident it's going the right way.

I know the ICANN organization also when you discuss these matters with them, they kind of raise awareness of are we accountable each and every employee? I think that's also a very important part of it.

MATHIEU WEILL: I think we're turning around the notion of trust, which basically is the seam of this ICANN 50 Meeting. We've heard trust at least as much as accountability and [that says] something. Probably more than transparency, actually.

And when I hear our proposals recourse and accessibility of mechanisms, the question for me is are we really addressing – and the pun is intended – the root cause of the lack of trust within ICANN or are we missing something? Is there something that you feel in your respective communities that we might have a blind spot on? It's a typical strategy. You think of what you know and you forget the blind spots.

So I'd like to see if any of you maybe has a perspective on something that us within the community we would forget, but it's important for people outside. That's elaborating on Lise's perspective.

In a way, Axel mentioned the fact that as long as there's the U.S. government, there may be suspicion. Are there any other outside aspects that could actually impact trust within the multi-stakeholder or ICANN model that we should not forget in the process? Chuck?

CHUCK GOMES: First of all, we have to have trust in the bottom-up multi-stakeholder model. We give a lot of lip service to this. The first thing, there has to be trust in that. And then that model has to be open and inclusive. It has to include processes that aren't only open to ICANN insiders, they need to be open broadly to those that are not yet in our community and may never be.

As long as we can continually improve in that aspect, those that are outside of our community will begin to have more trust in the model that we're very familiar with and that we use fairly effectively.

MATHIEU WEILL: So your perspective is that promoting the multi-stakeholder model, make it more inclusive, is one of the key aspects.

CHUCK GOMES: I think we do a pretty good job of trying to be inclusive. Like Kathy said in some of her earlier comments, we can continually improve on that. And it's not just promoting. Promoting the multi-stakeholder model is not enough. We do that pretty well. We all give it a lot of lip service.

But take, for example, the situation we're in right now. We have a couple processes – the IANA transition, the general accountability issue. Let's take advantage of the processes we have in place and use those to zero in on solutions like that and not come up with new processes to deal with that.

So in other words, trust the community to be able to do this.

MATHIEU WEILL: Kathy?

KATHY BROWN: So I think it's worth thinking about the word trust her. So trust could be a personal trust, it could be a familial trust, it could be trust in a process, trust in an institution, trust in a way of doing business, right? So what is it we're really talking about here when we talk about trust?

There's a couple of levels here. So the process we're talking about, the multi-stakeholder process, in part is to create the tools or the

mechanisms that allow work to go forward in a transparent way that people trust the way the work is proceeding.

And if there's a dispute, the trust comes in that the dispute will be dealt with fairly. Now, the dispute may not involve the whole of the community to decide the answer. The whole of the community may have decided how to decide the answer and has trust in that process.

And I think it's worth parsing this out because it's hugely important. If we're going to actually govern ourselves, then we have to understand the tools, the mechanisms, of governance and then put our minds to how to get those mechanisms trustworthy not only by us but by people outside so when they look, they say, "Of course. That makes sense."

And by the way, if that decision went that way, it's going to be hard to shake it because it was done in such a way as to be as right as it could be.

So this is actually I think, to me, quite fascinating to find a community that's willing to wrestle with this, but it's also not easy in terms of understanding what in the end will ensure trust.

MATHIEU WEILL: Do you want to open the floor?

KEITH DAVIDSON: I think so. We're into our last 15 minutes, so if there are questions from the floor, please raise your hand and we'll run a microphone to you. And if there aren't questions from the floor, I'm sure our interviewers will have some more.

BECKY BURR: I suspect there are questions from the floor.

KEITH DAVIDSON: Are there?

BECKY BURR: Who's going to be the first questioner here?

UNIDENTIFIED MALE: Hi, everyone. I'm [inaudible] from CENTR. One of the things I consistently keep on hearing through debates is that the NTIA is at the moment a backstop. They provide some form of – what was it? Appeal and recourse mechanisms in a final instance.

I'm not sure they do. And so what I'm wondering is if we're not making things more complicated by adding a wish list of things that we would really like now in a future scenario – and it might help I think if we keep those two separate, obviously to avoid, I think as Chris mentioned this morning or somebody mentioned this morning during the Board ccNSO meeting, that at the end of the process we need to make sure that we took into account everything that was relevant like the work done by the FOI Working Group.

But at least that we keep our wish list separate from what is essentially in this process.

BECKY BURR: So I'm going to ask Chuck to talk about that. I think what I've heard is people talking about the [U.S. NTIA] as a backstop. We've also talked about the need for recourse and redress. Put those two things together for us, Chuck.

CHUCK GOMES: Well, first of all I agree with you that I don't see NTIA as an appeal body. At the same time, I think we need one. Even going back to the ATRT reviews, both of them dealt with the independent review mechanism. Both of them made significant recommendations in that regard, and obviously the latest one is still to be acted on. That process is underway.

But still, we don't have that effective independent review mechanism I think in many of our opinions, and there may be divergence in those.

So the fact that NTIA wasn't an appeal mechanism, I don't think we should conclude then that we shouldn't add that to the mix of things as we're looking at accountability. I think it is really needed.

You're right. We should make it as simple and straightforward and understandable as possible, but it may be adding something new to the mix. And in fact, I think where it gets complicated maybe is that ICANN's governance model to date, from the very beginning, really isn't designed for that truly independent accountability thing.

So that may be one of the biggest challenges we have in coming up with solutions is changing that governance model that's been pretty entrenched from the very beginning.

BECKY BURR: Okay. We have a question over here from Oscor.

OSCAR ROBLES: Thank you, Becky. Oscar Robles from .mx. We made some comments [at the] ccNSO to the long-term planning processes 2015, 2020 I guess. I don't remember exactly the timeframe of this new plan.

One of the points we made there is that accountability thinks – is kind of hiding in the 5.2 objective, which is kind of a very low priority from my point of view.

And I think that if an organization like ICANN needs to work in the accountability process, it has to be very high priority in the strategic plan. Rather than a 5.2, it should be – I don't know – in the mission, vision or the various strategic goals with a lot of objectives going to the same thing of accountability. It has to [inaudible] accountability everywhere, not only in a very specific low-priority goal.

BECKY BURR: So that's the DNA. Accountability as DNA question. Anybody want to comment on that?

MATHIEU WEILL: Maybe more a comment than a question. Theresa [inaudible]?

THERESA SWINEHART: Yeah. You're actually telepathic. I was thinking there's an inherent obviously within the organization and that accountability is part of the

DNA. There's the bylaws and there's the AOC and there's various aspects.

But I hear your point that it's a given that the organization needs to be governed well and have accountability to the broader community and that's a given that's inherent, and that is obviously an underlying aspect of the entire strategic plan and its operations overall.

But I hear what you're saying as well. [One] wants to put that as a front-and-center overarching principle of any strategic area. So that's a very useful comment to make sure that's captured right at the beginning as one of the overarching aspects of a strategic plan as well. Thank you.

BECKY BURR: Others? Questions?

UNIDENTIFIED MALE: Looking at the IANA transition, I feel that the transition is a rather small kind of thing and that it's mostly clerical and technically based. If that is true, then accountability for that part could be achieved just by setting up service level agreements and that will do the job.

What would be left open is – and we are viscously discussing that – redelegations and delegations. I'm on the side of – especially for the ccs – nobody should care about redelegations for the ccs. So we're just talking about delegations.

And then accountability for just a delegation process, well, is it really that big kind of thing we're currently talking about? I suppose not.

And then I'm sure we do need accountability, but accountability for a body that is much broader and wider than the one we are currently talking about, because we're talking about setting up a body that is responsible for driving the Internet in the future. And ICANN is just a rather small part of that.

So we should stop talking about ICANN' responsibility or accountability and I think we should start about designing a body and talking about accountability for that larger body, because as I said, for the transition process accountability seems to be rather small for me.

MATHIEU WEILL: Anyone want to respond on this comment?

UNIDENTIFIED FEMALE: I was with you until you said we needed to set up another body. You know, you get into this wider conversation about Internet governance, which is happening all over the place, how you're accountable for various things that are happening in the Internet space and that's a whole different conversation where I do not think we need to set up some other new body. I think we actually have a lot of mechanisms that are at work right now that we probably need to identify.

But I did want to associate myself with your comments in the beginning, that let's look at each piece of what happens in the IANA function, figure out are there mechanisms for both policy making, review and redress should there be an issue, and do it methodically and go through.

And when you do that, I think you get to a much more specific place around whether and what kind of tools you need to ensure that.

CHUCK GOMES: And let me respond as well. I agree with you that the IANA functions are pretty straightforward and they're operating quite well. But if there is an instance where something is needed, we need to have the mechanisms for that. Hopefully, like you heard me say before, that won't be needed very much and maybe even less so on the IANA side than in the broader side. I think we all get that, but you still need that.

In fact, one of the comments that I think has been quite prevalent coming from just about every sector in the ICANN community is that the general accountability issue needs to be resolved before the transition happens.

Now, I think we can still do that in a timely manner and that's good and that's the goal we should be shooting for. But even if it's only something totally unknown that might happen with one of the pretty straightforward IANA functions, if you need that appeal mechanism, that redress mechanism, it should be in place. Hopefully you don't need it.

BYRON HOLLAND: Byron Holland, .ca. I'm not going to talk about trust, transparency, or accountability. I'm going to go strictly to a process question for Theresa.

As a community, if we are not able to select our four people by middle of next week, how much of a problem is that going to be if we need a little more time?

THERESA SWINEHART: That was definitely [inaudible] on the spot. I would encourage to get them identified as soon as possible right after that. As I mentioned, we have already, through the submission process – and you're referring to the Coordination Group, my bad, to the Coordination Group itself – as mentioned, some names have already come in through the submission process and I would expect more names to be coming in over time.

So obviously, those names that come in after that date would be added on to the group as soon as they're provided. Again, the group will try to convene in the middle of July to focus in on the work program and how they're going to operate. And so obviously that would be an important opportunity. But again, as soon as possible. Again, names are already starting to come in.

UNIDENTIFIED FEMALE: While you're on the topic of process or process, do you have a sense of timing on when you expect to respond to the accountability comments? I realize the comment period isn't closed, but giving us advanced warning.

THERESA SWINEHART: Yes. First of all, the comment period has not closed yet. And second of all, it will depend up on the amount of comments coming in and then

allowing enough time to do that in order to also show all the feedback that has been received.

So I'm a bit reluctant to put myself on a defined timeframe, but I would certainly give it a couple weeks in order to allow that time. But as soon as we get it in, I will look at getting an indication out to the community so we can have an expectation. But I'd say two to three weeks would be a good guess.

CHUCK GOMES: Fadi told us all, and I know that Theresa supports this as well, that this process is not driven by ICANN staff. It's driven by the community. And so let's keep that in mind. I don't think we should stretch it out a long time, Byron, in terms of getting – and we're working on it, too. Let's do it in a timely manner, but let's also remember that it's us that's driving this process and ICANN staff is providing tremendously valuable support for us, but let's drive it and make sure that that Coordinating Group works into the multi-stakeholder model and the processes that we develop.

And if we need to tweak it, let's tweak it. It actually looks like it has a lot of value, but it's us that's driving the process, not ICANN staff, and they have said that themselves.

MATHIEU WEILL: Keith for a conclusion?

KEITH DAVIDSON: We're right on time, but if there's one more burning question from anyone, I'm sure we could accommodate. If not…

MATHIEU WEILL: You had it arranged with [inaudible] I guess.

UNIDENTIFIED MALE: If I could have the shortest answer possible from each of you, what is the one thing that you most fear as an outcome of this process? Good luck. Should we start with maybe Lise?

LISE FUHR: Well, actually I fear most that we get an outcome that's only supported by ICANN and not the whole Internet community worldwide.

UNIDENTIFIED MALE: Axel, would you follow up?

AXEL PAWLICK: Yep. I agree with that. And basically failure of the process and no outcome for the foreseeable future.

UNIDENTIFIED MALE: Chuck?

CHUCK GOMES: I think my biggest fear is we'll go through a lot of exercise and we won't have any meaningful change, that it's just basically status quo and we

haven't solved any of these problems. That may be saying that Axel just said. Most of you have heard the thing "the more we change, the more we stay the same." I'd really like to see meaningful change.

[KATHY BROWN]: So we made a big bet on this multi-stakeholder process about what 20-something, 30 years ago and it's worked. It's really worked. We've actually taken it amongst ourselves as users of the Internet and we've made it work.

And ICANN has been along the way up and down, and it struggles back and forth but it's made it work. And my biggest fear is that there are those who want to say that this kind of process, this kind of bottom-up, non-regulated, non-governmental way of doing business can't work. My biggest fear is that we fail and that it has ripple effects that are quite profound.

MATHIEU WEILL: So, [inaudible], you can conclude and then Byron wants to say a word. Oh, Theresa.

THERESA SWINEHART: I have to say what I fear.

MATHIEU WEILL: You're a wonderful, valuable support. You have the floor as well.

THERESA SWINEHART: No, no, no. I just have to say what I fear. To add on to the points that have made here, we've seen the evolution of the multi-stakeholder model whether it's in the ICANN context or the context of policy development by the regional Internet registries, IETF, any of the organizations. These processes are testing all of that. They're testing the dialogues amongst all the communities whether it's only the namespace or anything else.

It's a unique window of opportunity that we have with regards to this transition and this next phase, and I think my biggest fear is that as we're – not we as ICANN, but we as the broader community – looking to this as the multi-stakeholder model can truly step to the plate and show that this is the right way to find an important proposal, an important opportunity, to this next phase of the transition process.

So I think my biggest fear is that we don't see said opportunity and step to the plate for that, and that as we're getting tested, we of course will all need to be changing in ways that we might not have foreseen before but should be prepared to do so.

KEITH DAVIDSON: And with that, I think that brings us to a tidy point of ending for this session. So please join me in thanking the panelists and the interviewers for the session. I feel very well better informed than I did at the start of the session and I hope everybody in the room feels likewise.

Remember that tomorrow we have a further open discussion on the more particularly focusing on the transition, so please don't miss that.

And remember all ccTLDs, you are involved and engaged whether you feel that you should be or not. This does impact you.

But please join me in thanking the panel. It's been greatly appreciated.

[applause]

And now I'd like to hand back to Byron who has a housekeeping item or two.

BYRON HOLLAND: Yes. So thank you to the panel. That was very interesting. Strictly housekeeping right now. This is our lunch break. We have slightly less than an hour now, and after lunch at 2:00 we meet with the GAC and they are about as far away from us as you can possibly get in this hotel, so they're in the East Wing third floor down in the basement. So we need to be there at 2:00. After that meeting, there's a quick coffee break and then back here.

[break]

ANNE-MARIE EKLUND LÖWINDER: My name is Anne-Marie Eklund Löwinder. I'm from .sc and I will be the sharer of this session.

I just wanted to start to outline – there is no security policies, standards, guidelines, or procedures who can foresee all of the circumstances in which they are to be interpreted. Therefore, stakeholders are not grounded in a culture of security. There is a potential for improper actions. And the greatest benefit of having such a culture of security is

the effect it has on other dynamic interconnections within an enterprise. It leads to greater internal and external trust, consistency of results, easier compliance with laws and regulations, and greater value in the enterprise as a whole.

By my side, so far I have two – it should be three – excellent presenters and I think we should start with you, Simon. Would you like to introduce yourself?

SIMON MCCALLA: Good afternoon, everybody. I'm Simon McCalla. I'm the Chief Technology Officer at Nominet for .uk.

ANNE-MARIE EKLUND LÖWINDER: And Carlos?

CARLOS: Hi, my name is Carlos. I'm coming from NIC Mexico and I'm going to talk about some best practices for secure development environments.

ANNE-MARIE EKLUND LÖWINDER: Thank you. And we're also waiting for Dave Piscitello from ICANN who will hopefully arrive in time for his presentation. Anyway, Simon, please start: "UK Security Roadmap."

SIMON MCCALLA: Thank you. Good afternoon, everybody. So I'm going to very briefly talk for about ten minutes on looking at how Nominet has developed a security roadmap over the last year. In particular, some of the thoughts that went into creating a roadmap for registry, what does it mean? What kind of products and services could a registry offer? And then what has been the feedback from some of the stakeholders as we started to introduce those and announce those products?

We want to talk about where our security roadmap came from. It came from a number of areas that force us to start really thinking about this seriously. The first one was just a general increase in the desire for more security. We've had that from our government, we've had that for our stakeholder groups, and we've had that of course within the ICANN circles here. As many of you know, we've also recently launched registrations directly under .uk, and as part of the consultation, we started to say to many of our stakeholders, "We think this is a good opportunity to improve security in U.K. domains. We had some interesting and some challenging feedback when we introduced some of that.

We're also very much in the businesses – for those of you who have seen us presenting earlier on this week of innovating new products and services. When we looked at how were we going to innovate, what were we going to do, we said, "Actually, security is a very obvious area for us to work in." Plus also, there is a lot of existing initiatives within the business that were going on at the time that we have said, "Actually, we need to bring these together into a little bit more of a coherent framework that we can announce."

That's really the birth of our security roadmap. Who's the audience for this? Who are we trying to actually show this roadmap to? Actually, it's a pretty broad group. Firstly, and by no means the least, is our own staff, actually giving him a clear direction for what we were doing as a registry of our security was important.

Obviously, our registrars and our registrants, very important that we had a public position on some of the security aspects of the .uk but also [our wider] stakeholders and ultimately we hope out to consumers and other Internet users. And I think that's a very challenging part of what we're doing. But we hope ultimately that people will start to recognize some of the things we're doing inside .uk when they are browsing the web and they're shopping and they're surfing that they will actually think, "Oh, U.K. is a bit more secure than other domains." So that's something we hope to achieve.

So really, when we looked to bring this together, we looked at existing work we already had. We looked at, "How can we share data?" Many of you I'm sure have got systems with all sorts of interesting data and metrics. If you came to Tech Day, you would have seen us talk about some of the metrics we've been able to pull out of our DNS traffic. You can bring those together to start to inform some of your more consumer-facing-security products.

We extended some of our existing products and services that we're already working on inside the registry. We carried on using our R&D team to focus and say, "Right. Really, I want you to push the bar on this and make a difference. How can we innovate and create new products?"

So we looked at those for two reasons. One is to try and enhance the existing service to U.K. registrants but also, hopefully, we hope that we can deliver new products and services to the market that perhaps you might not have expected Nominet to be looking at in the past.

Apologies about the slide. The PDF has slightly truncated some of the words. We looked at six really key themes when we put together our security features. Security obviously is a big theme. But it goes into much more importantly – it's about trust, about people trusting the domain their visiting. It's about detection. It's about actually been able to detect stuff that is going on. So having technologies and tools that [later] detect. Behavior is really important.

It's resilience was the most important thing, particularly for our government is that .uk stays running and it stays running 100% of the time. What was coming along? What cyber attacks, DDoS, etc. that could derail a top level domain.

Then education and assistance. It's great having lots of technology behind your registry and it's great talking about technology, but ultimately if end users, registrants, even registrars don't understand some of those security themes, then you need to put quite a bit of work into educating people.

Enough of the themes. Again, apologies for the slides being slightly messed around with. We looked at – this is our sort of wall of products, if you like. And it's quite significant. I'm not going to go through all of these in turn, but just to say if you take a look on the left-hand side of the slide, you have the Internet users and their real needs are

understanding education, understanding what's going on. Just making sure that the person they visit, the website they visit it's the real registrant. Understanding some of the terms, worrying about articles in the news about malware. So very much in the advice and education side.

As you go across from the right side to the left, you're getting into small businesses, people a bit more web savvy, they've got very different needs. They want to understand security a little bit more deeply. If they are registrants or somebody holding a portfolio of domains, how do they secure their domains more securely? If they're having problems with their business online, how might we help from there?

Also, we are now looking at something we call domain reputation scoring, so we are starting to score domains by how clean or how dirty they are in terms of security features. That's very controversial, but we believe it's going to make a big difference to how people work with domains in the future.

As you go over to the far side, the far left-hand side of the slide, we've got the much more technology-focused products and services. You may have seen us talking about our advanced DNS analytics talk of Bumblebee. So we're mining – we're looking at DNS data in detail. We're looking at every single packet. We're looking for issues and challenges. And then we're looking at those packets compared to others. We are looking for – we are spotting botnets. We are spotting malware. We are spotting DNS misuse, criminal behavior. We can start to tackle that once we can see those patterns. If anybody is interested in understanding how we're doing that, we're very happy to talk. But

we've had some real successes with law enforcement in tackling crime just by looking at patterns in DNS.

So to try to break down by themes of what we're doing. In terms of our register data, just for the data that we hold – we're doing three key things at the moment. One is we have the data quality program ongoing at Nominet. We are looking at the quality of the data, making sure our registry is as accurate as possible. Where we find it isn't accurate, we try and fix that. We're validating and verifying registrants. Again, that is quite controversial. We are in process of taking out domains and canceling them if we cannot contact the registrant and the registrant data does not look correct.

We're also extending our WHOIS and our registry search services to allow it to make it easier to find, make it easy to search, and to search on additional features. For example, the right of first refusal for these new .uk domains. We're doing a whole chunk of work around building trust in the data that we hold as registry.

We then look at security of our registry and our register. We're doing three things there. Firstly, like many of you have a domain locking service. So we have offered the ability for our registrars to lock portfolios of domains, add additional security feature so that they are not – they [inaudible] of a social engineering attack as we've seen in a number of registries in the past. So we have a domain locking product which had some good take up.

You probably heard me talk about this before in meetings past, but we spend quite a bit of time educating our staff to avoid being victims of

social engineering attacks. We do get attacks at Nominet. We get people ringing up pretending to be registrars, pretending to be registrants, attempting to get details changed on the register. And they're getting very, very clever doing it and the attacks are becoming more sophisticated. So we train the staff to recognize when somebody is trying to con them out in giving some data that they wouldn't normally give. That's been very successful.

We are also introducing this summer two-factor authentication for our registrars. So for those who want to access our online services, they will have additional security measures. They'd like to have that. Again, we hope that that prevents some of the more sophisticated attacks that we see in the past and will also help prevent some of the social engineering attacks that we've seen.

We move on to DNS security itself. We, like many of you, offer DNSSEC and have been doing that for a long time. Take up in the U.K. is very poor. We recognize that where we're seeing significant success such as in .nl and we're offering a DNSSEC, offering a discount on registrations makes a big difference. We currently don't do that, and as a result, DNSSEC take up is pretty slow. But we are starting to see more people validate. We are seeing some interest from the ISP, so we hope that that will grow and we're looking at other ways to increase the penetration of DNSSEC.

Again, we also look very, very closely at DNS traffic. We find incredible [stuff] inside the DNS and strongly recommend that that's an area to look at because if you're serious about tackling security in your registry and you're serious about tackling the DNS in your country then your

DNS data holds a lot of clues to how to tackle some of the quite significant issues we see.

Education assistance. We're doing two initiatives along on that front. We have initiative that we are piloting this summer called Cyber Assist. Cyber Assist is a service aimed at the 3 million plus small businesses in the U.K. who find dealing with some of the cyber challenges very difficult. They are one, two, three-person businesses who don't have an IT expert on their team. When they suddenly find that they can't access their e-mail or they have got a virus on their computer, who do they turn to?

Our research has shown that actually people find it very difficult to navigate that space and understand what to do. So we're offering a service – a pilot service I should say – to businesses in the U.K. We're launching that in a couple of weeks' time and I think we'll see some interesting results from that. That is a phone service. It's an online service too. We're offering direct support to customers.

Finally, we have a website called NovaNet and that's our education portal which is right across the U.K. It's a very, very popular site and we publish articles about – you may have heard about this latest malware or what's this Heartbleed bug thing about. We put articles on there to help try and make that a little easier for consumers and customers to understand.

Then finally, we look again at innovation. I think this is a really important place. We are investing very, very heavily at Nominet in innovation and research and development. We recognize there are gaps

in the market for tools and technologies to help registries. We recognize that DNS… Steve Crocker once said – he's a bit of a technology cul-de-sac and consequently, a lot of the main vendors don't provide DNS security products. So we're looking to innovate and to create new products and services in that space.

But I urge all of you, if you've got a technical team, use their skills because some of the things that they can do with your data can have a really big impact on the security of your registry.

As I said before, we're doing domain reputation scoring which is controversial but is producing some really, really interesting results. And we've been really surprised by what we found and we've been surprised that some of our worst domains are in the U.K. but also where some of our best domains are. And so, we're able now to analyze the whole register and look and see where the bad guys are and see where the good guys are.

So just a quick set of observations and lessons from doing this over the last year and a half. I think you've got to innovate to stay current. We have to change and adapt to the world that's around us in terms of cyber threats. It can be a real opportunity if you're a registry, particularly if you're a public purpose registry like so many of us are, to publicize the existing good work you're doing and to be much more open about how serious it is to take security and take these threats. It's an opportunity to provide your registries with the ability to compete and diversify.

As I said, there aren't that many products out there, and actually, if you create products and services, people are really interested. We've been amazed at the amount of interest we've had in some of our services this week. It also gives you a great ability to build broader outreach to your stakeholders. The U.K. government has been really interested in the work we're doing. There's been an amazing amount of feedback in terms of some of some of the stuff that Nominet is getting out to and say, "Wow, you really are stepping it up to the plate. We're not seeing this in other sectors. We're not seeing the ISPs taking this seriously as the registry is taking it." It's a great opportunity for you.

There is a downside to doing this. Not everybody welcomes the fact that registry has been taking part in improving security. There are many people who want to sell domains very cheaply, very quickly, and they want to get them out to market. I totally understand that need. And this is where being commercial and acting in the public interest can sometimes [grate] together.

I think many of you will probably have that same challenge. The more security products you put in there and the more stringent you make your registry, the louder some people will complain at you. The happier some people will be as well I might add. But we have taken our fair share of criticism for some of the steps that we've taken. We had to back away from some security services and products because our registrar channel have found them too challenging to implement. So you have to take a measured approach to doing this.

Some people see registries reaching into the security field as a threat too. They don't want us playing in this space. They don't think we have

the right credentials to provide security products. So it can be challenging when you're saying, “We have a new product and we think it could make a huge difference.” Some people will come back with a reaction, “Why are you doing this?”

In general, that move in terms of diversifying and moving not just from servicing DNS and being a DNS registry but providing products and services can also be challenging as well. And we’ve had a few people say to us, “Can’t I just stick to running .uk and leave security products to somebody else to do?” Our answer to that is “No, we don’t believe that’s right. We believe we should take part in this, but that can be challenging.” Thank you. That’s it for me.

ANNE-MARIE EKLUND LÖWINDER: Thank you, Simon. We do probably have time for a quick question if someone is very eager to put one. Nope. Not yet. Okay. So we turn to our next speaker who will be Carlos Alberto Cárdenas from .mx who will talk about secure software development, which is another interesting area.

CARLOS ALBERTO CÁRDENAS: Okay, I’m going to start. My name is Carlos. I’m coming from NIC Mexico. I’m going to show you what we consider to be some good practices about how to secure the software development environment. Well, I’m going to go a little bit fast because I have several slides. Okay, thanks.

We have a set of homemade applications at the core of the software infrastructure. That process information coming from intranets, extranets, and requests from our registrars, and all of those requests are interacting with one or more databases and update the SUM files on the DNS master server which spread all those changes throughout the whole network of the DNS slaves that are going to answer the end user requests.

We have two main environments that we call the development environment where applications are tested and modified, and another one called the production environment where applications are released.

So we have more than 40 applications on the development and more than 120 application instances on the production. This is because of the sake of redundance that we have so many instances on production. In fact, we have several redundant measures. It means we have many applications on many servers, on many devices, on many data centers for the sake of redundance. If something fails, if something goes – it's okay all the time.

So we have a team integrated for 30 people including developers and visitors who have access to the DEV environment. I'm going to show you. All possible risks we have is that those developers and visitors could take code from inside the company to outside and do wrong things with it, unauthorized access to the sensitive data from our customers, and passwords that applications use to be compromised. Let's see, what are we doing for keeping that secure?

We have many security measures in order to secure code. It means no one can take what we are doing to outside the company. And securing data – it means our customers could be okay. It could be nice. We are doing the right things with their personal data. And secure password means that all of our applications are going to be safe to access the resources just by the people allowed.

All the code is stored in the DEV servers where developers can access through their laptops that have several security policies that just allow to connect through a remote desktop connection and don't allow any other copy actions.

Okay. The access to those servers is also restricted. First of all, the developers have to authenticate against a VPN. It could be from inside enterprise or from Internet. After that, we have several separated networks on routers and different VLANs on switches. This is the network layer of security.

After that, we have some rules on firewalls that only allow remote desktop connections. It means nothing be taken from inside those servers to the outside. This is for code protection. And regarding data protection, every time we release a update to the production environment, testers need a fresh copy of the database from the production environment to the development one. So, sensitive data should be replaced with dummy data so testers never have access to the personal information. The main advantage is that the code is always safe and data protected. And the access is also restricted.

Let's see now what we're doing for the sake of having secure passwords. When application needs to access a resource such as a database or it could be a web server or something else, it needs a username and a password. For passwords, we have many kinds of authenticator certificate phrases, password for authentication for authenticating on a provider service and that must be protected.

Where are we going to store those passwords? Well, we can do it in a flat text file. However, it is not very safe. One step forward, we can think of storing it in an encrypted file on the file system and ask for the credentials at the moment the application starts. It is better than the one before. However, if we think that we have many servers – more than 50 servers – it is hard to administrate. So, we are thinking that the best practice could be [to] have a centralized application that could provide all those credentials to the other applications, so it is easy to administrate and hard to steal. This is just one point of administration and it is the weakest part of this mechanism because it is also one [just] point of failure. If we have that application in several instances, there should not be problem with it.

Let's see how it works. We call it the CIS for Credential Information Service. That service provides credentials to all other applications. It means when an application needs to connect to a database, it asks the CIS for a password. The CIS gets that password, decrypts it, and returns it back to the application that now can connect to the resource. However, the CIS doesn't know anything about passwords. He only has the master key needed for decrypting the credentials.

Credentials are stored in another database where [they] are stored in an encrypted way. When the CIS starts, a master phrase is needed to be entered by the administrator. So it is going to be used for decrypting the credentials and it is always loaded in memory.

This slide shows us how the CIS can serve many credentials to many applications. The main strength of this mechanism consists in the protected master key that the CIS has and the encrypted credentials that are stored on the secure database. Also, we can see the application channel between application and the CIS is also encrypted. It means that when an application needs a password, it has to authenticate first. After that, all traffic is encrypted.

What will happen if a credential will be compromised? Well, the only problem will be to update that record on the database. This has happened several times and it is relatively easy to change it. There is just one place where to change passwords.

So what if one system administrator leaves the company? Well, here the scenario is a little bit different because the master key needs to be changed as well and all credentials too. So a new master phrase must be stored.

Finally, the main advantages of the system is that there is only one point of failure that nobody knows what passwords are and it is easy to change in the case of someone leaves the company.

I guess that is all for my part. Okay, I want to say before to finish those practices are just a brief of what it is being done at NIC Mexico for

enforcing security on the applications. I hope it could be helpful for you and I appreciate all your questions. Thank you.

ANNE-MARIE EKLUND LÖWINDER: Thank you, Carlos. Any questions? No. So, thank you very much. It's a very interesting approach. I will turn to our third speaker, Dave Piscitello from ICANN. Welcome. Would you mind starting to introduce yourself?

DAVE PISCITELLO: I'm Dave Piscitello, Vice President of Security and ICT Coordination at ICANN. First, let me thank you for having me come and talk with you today. I haven't been here for a number of years and I see some familiar faces. But I think I'll go right into this because I know your schedules are always very, very tight.

For a number of years and evolving from work that some of the Security team have been involved in with various aspects of what we call threat awareness and preparedness inside ICANN of threats to the DNS and threats to the SSR in particular. Law enforcement are steadily growing into what we now call a public safety community which goes beyond law enforcement into ministerial levels at various governments. Jurists, prosecutors, Crown Counsels and the like have been asking us, "Help us understand the DNS. Help us understand how people are misusing the DNS, how they're abusing the DNS."

So it began with a 30-minute talk that evolved to a two-hour talk. It evolved to a four-hour talk. It evolved to "Can you do this in two hours

to six hours? Can you do some hands-on? Can you do some demonstrations?"

So over time we developed a training program that we now call "Investigating DNS Abuse and Misuse." The purpose of coming here today is to basically talk to you about this program, because in some cases there's been some misconceptions about what we do. I want to make certain that people actually understand it and encourage you if your community is interested or there are people that you might now who would be interested in having us come do this before you would be happy to.

What I'd like to do is invite Steve Conte for just one moment before I start and just have him give you an overview of the presentations and various training programs that we are now offering. I think some of you are familiar with some of his portfolio, but he can tell you today what we are talking about as a new program perhaps to you and some of our plans for future programs.

STEVE CONTE: Thanks. I was hoping to stand up so you guys could see my face but I'll duck instead. I've been involved with ICANN – actually, this is my second time now. I was here from 2002-2008. I recognize many of you and many new faces here too. I recently rejoined ICANN and working with John and Dave in the Security and Stability Resiliency Group to coordinate the trainings.

So as you know, we've been providing training since about 2003 on registry operations and we've been moving into DNSSEC and things like

that. We're trying to take a more holistic and strategic approach with training and get in there to regions to the community on a less of a reactionary level and more of a strategic level.

So I just want to take a moment and show my face and say if there's an event that's taking place in your region, please talk to me. I'm going to be around all week and I'll be here during the coffee break and stuff. Speak to your regional vice president from ICANN and we can start coordinating things. We want to get out there. We have an increased staff. We have some new programs which Dave will go over.

My ask to the community here is, since a lot of what we've been doing since 2003 and, in some cases, 2008 on some programs, what are we missing? What can we be training that's relevant to the SSR that we're not doing yet? And I really look forward to hearing from the community what we could be providing to your constituents and to your community as well. With that, Dave, I'm going to turn it back over to you then. But thank you for your time.

DAVE PISCITELLO: Thank you, Steve. I think many of you are familiar with the first three programs that registry or TLD operations and the Secure Registry Operations or what's commonly known as SROC in the community and then Rick Lamb's training programs that help various people understand how to implement DNSSEC at the top level.

What I'm going to talk about today is the investigating DNS Abuse and Misuse Program. We have two programs that we're probably going to try to put together over the next summer. They are requests for security

awareness programs for ICT users. I distinguish ICT end users from consumer end users by the fact that they typically not only have to worry about things like protection of their own personal information, but protection of a corporate or government information. So understanding how to do both. And many of you probably heard terms like “bring your own device” or BYOD. We’ll be talking about things like that and some of the ways that we’ll inform people on how to become good digital citizens not only for themselves but for their organizations.

The second is actually for ICT administrators. And this is for the people who have to manage the people who are ICT end users. We’ll probably have more to say about that in L.A. and if you’d like to have us come back at some point and talk to you about those, we’d be happy to do so.

What we’re going to discuss today is the purpose of this investigating DNS course and what the topics we cover when we present this course, who gets to participate, what are “investigative methodology” is and what kind of resources we share.

The purpose of the training is to assist the participants and understanding a number of things that are probably familiar to almost all of you here, but when you go to a law enforcement office and agents who have been in the field for many years and now are finding that they need to go from what they call meatspace into Internet space and now prosecute or investigate crimes that are involving things like counterfeit goods, illegal pharmaceuticals, child abuse, spam, phishing, identity theft – all that no longer happens just in the real world or just in the Internet. There’s a lot of crossover.

So there's all sorts of activities that are facilitated by the Internet but ultimately there are real people committing the crimes, there are real people who are acting as mules to go and get money from one place and put it into another, processing and delivering goods.

So there's a lot of information and intelligence that law enforcement now have to collect during the course of an investigation. And many of them are not prepared. They don't know what the DNS is. They don't know what a registry operator is. They don't know the difference between a registrar and a registry. They think it's all ICANN and they come to us and that's not a very useful place to go most of the time. This was sort of a self-preservation course. If we don't teach them this, all we're going to do is answer things like sealed court orders that we can't execute on because we're not the party.

The things that we cover are name registration and DNS system operations. We talk about the registration ecosystem for both the gTLDs and the ccTLDs and explain the differences and the different organizations that the service organization that served them.

And then we go, after that background, into an overview of the different kinds of criminal uses of DNS and of misuses of domain names. The rest of the course is really helping investigators see that investigating crimes that take advantage of the DNS is no different from the way that they would go about conducting an investigation. The tools are just different. So we don't try to teach them a new methodology. We try to say that "Here's your methodology and here are the tools you use instead of your notebook and your flat fee."

We focus primarily on identifier systems and we focus primarily on domain names, registration information, IP addresses, autonomous system numbers and their registrations. But we also help them understand how to take a domain as a starting point or URL as a starting point and find what I tend to call “bad neighborhoods.”

For example, a name server that is hosting not just the domain they're looking at but maybe 1000 bride sites or 500 counterfeit good sites. And so we show them that there’s links between all these and we try to help them not only look at one part of the puzzle, but piece together the entire picture.

To do this – and I think probably some of you have actually done this kind of investigation within your own registry or your own country – you need to look at zone data. You need to look at domain registration data, DNS traffic, authoritative name servers and resolvers, addresses and routes, understanding who’s hosting. Those are some of the bases that we give them and explain to them how to fins this information.

The other thing that invariable comes into play especially in a world where we’re just besieged with malware is understanding how to do content analysis, understanding how to look at and see whether some actors that they’ve already identified already have bad reputations.

One of the things that we try to emphasize and it’s always helpful for law enforcement is that we try to use and show them publicly available services, especially services where they don’t have necessarily revealed the fact that they're doing an investigation.

One of the things that's hard for a law enforcement is that if the criminal actually knows that law enforcement is studying them or has them as a person of interest, then the criminal might behave differently. So we explain how proceed anonymously, how to use public resources, even how to use addresses that are not necessarily known addresses assigned to Interpol or Europol and things like that.

We primarily use the DNS, other sources of DNS, sources like WHOIS. We show them a lot of web-based services that had been developed by the security and operations communities to do research. Then we actually try to introduce them to what we call the trust-based collaborative communities, operations communities, communities where security researchers and investigators and law enforcement collaborate under some sort of vetted or credentialed environment. And we essentially say, "This is the pool of information you can use. This is where you go and you conduct the investigation."

ANNE-MARIE EKLUND LÖWINDER: Sorry, Dave. We are soon getting into the coffee break so can you make it a bit short?

DAVE PISCITELLO: How many minutes?

ANNE-MARIE EKLUND LÖWINDER: None. Sort of.

DAVE PISCITELLO: Well, I mean I can stop if you'd like me to stop.

ANNE-MARIE EKLUND LÖWINDER: [inaudible].

DAVE PISCITELLO: Okay, thank you. I'm not going to go through this whole slide because obviously it's very long and I'll make certain that you all have copies. The philosophy of the course is essentially tell law enforcement the proceeding is just like trying to match a fingerprint with a fingerprint you've pulled off at a criminal site. How many points or markers on the fingerprint you have actually dictates the quality of the match. So only two matches is not very good, ten is much better.

The markers that we look for when we were doing these kinds of investigations include the checks that I've listed here. I'm going to skip participation because I already mentioned that. But the kinds of resources that we show and share – and, in fact, I can point you to a site where I've got all these on a single page where you can actually try them all – is things like domain tools, DNS tools, ARIN WHOIS, various WHOIS services and applications.

We go and we show people how to pull website content without executing the content by using things like cURL and Wget. We show them how to upload suspicious executables or JavaScripts or URLs to places that will do malware analysis. We then show them how to actually parse mail headers to look for direct-to-MX spam to look for various other kinds of spam campaign techniques. And then at the end,

what I do – and I'm training other people in different regions to do this as well – is we walk them through scenarios and case studies.

Literally, I wake up in the morning before I teach. I grab something out of my spam folder, I get several domains, and for the day we walk through those. Or sometimes there's someone in the room who actually has an IP address or a domain that they're investigating. We conduct the investigation in real time, so they get a really, really good hands-on exposure to all these tools. And by the end of usually four to six hours, you have all these little things clicking in their heads going, "Oh, this is just like what I do. All I needed was the right set of tools."

I'm sorry that we ran a little bit late. Again, if you have questions about this, you all know how to get in touch with me. I've been here for many, many years. If you're interested in the URL for the page that I just described, it's got about 30 different kinds of just launch applications to go and use some of these tools. It's actually very handy and I have lots of people who use it. The only thing I ask you to do is not share it on a public list because I don't want it to be DDoSed. But thank you very much.

ANNE-MARIE EKLUND LÖWINDER: Thank you, Dave. Very well picked up in the end. So I'm sorry for the notice earlier.

Anyway, that is the end of the security session we started with pointing out the importance of the culture of security. And to fully understand the information security that it is important, one needs to understand

both the value of the information and the consequences of such information being compromised.

So I think we have proven this right. I know that a lot of ccTLDs are working very hard to improve the information security work and we all need to remember the RFC 1591. We actually live on trust, and so we better do this well. Thank you very much. Enjoy your coffee break.

UNIDENTIFIED FEMALE: Dear colleagues, we're getting to the last session of our agenda today. And now we have IANA update presented by Kim Davies. So, Kim, the floor is yours.

KIM DAVIES: Thanks very much. This is the IANA update for ICANN 50. Three topics today. Quick review about processing statistics. I want to talk about trusted community representatives and then about evolving the root zone management system.

I think I spent a lot of time at the last few meetings talking about our SLAs and KPIs and stats and showing you a bunch of graphs. So rather than bore you with it this time, I'll just show you just some real quick snapshots for those that haven't been at recent meetings. We have a much expanded session on the IANA website dealing with performance standards. If you want to look at a lot of statistics, SLAs and so on, we post a bunch of monthly reports there now. They go back about six or eight months and we update that every month.

But just real quick, of all the different types of root processing, the average is between four to seven days per type. The one exception there is root server update. We did one of those. Changing the root server itself is a little more complicated, so it takes a little longer.

SLA performance for the last month, 100%. That either means SLAs are too easy or we're doing quite well. So I'll let you be the judge of that.

Okay. Moving on to trusted community representation. For those that are not aware, every three months, we do what we call a DNSSEC Key Ceremony. Essentially what happens is we have a bunch of experts from around the WorldCom to a windowless room. We perform a ceremony where we take out the DNSSEC private key for the Root Zone. We use that to generate three months' worth of operational keys and those operational keys are then used to sign the Root Zone on a daily basis.

Doing this in a secure way in a trusted way is a key part of security of the DNSSEC system as a whole. It's essential to us that we have a process that is well trusted by the community. And because these trusted community representatives – these experts that come to witness the event – are such a crucial part of how we operate, their participation is important and sustaining their participation is important.

So we've been doing the ceremonies for almost five years now. Some of the representatives that have been involved since they won had suggested some tweaks to the way we operate the program. We thought it was a good time to consult with the community on how we have that trusted community representation. So a few months ago, we

did a public consultation. We asked for feedback on how that aspect of the ceremony is being conducted.

Just an additional bit of background, there's a pool of experts. The pool is right now about 18 or 19 people deep. Of those 19 or so people, there's two groups of seven. One assigned to the West Coast of the U.S., one assigned to the East Coast of the U.S. The remaining few are backups. And of those seven for each facility, every time we do a ceremony, we need three of them to attend. So in the space of a year, a lot of these people are coming at least once, sometimes twice or maybe even more times per year.

So we did a consultation. The net result of the consultation firstly is that until now these representatives have come on their own dime. When we solicited for volunteers in 2010, it was on the basis that if you volunteer, you're able to pay your cost of attending. Based on the feedback we received, we're now looking at ICANN funding travel cost to come to these ceremonies. This has an additional side-effect that I think a lot of people that were interested in being experts that participate in these who are otherwise inhibited by cost reasons are now potentially people who have the ability to participate.

Second item is we'll implement term limits and rotate the existing TCRs. As I mentioned, they've been doing it for almost five years. This seems to be general consensus that it's appropriate that we find a mechanism to bring new blood in. So we will implement some mechanism by which we'll rotate the TCRs.

We'll clarify how we select those TCRs and what their obligations are, including what the minimum level of participation is. We also plan to implement a new security system for our key management facilities. One nice side-effect of this is that – I mentioned that that number seven. The seven is really sort of a technical limit to the number of TCRs we can have based on the design of the security model. With a new security system, we can up that, which means that even though we still need around three people to participate, we can pull from a larger pool of people which will make operating these ceremonies a bit easier.

An open question for this group is: where should we solicit new volunteers from? I think having the trust of the ccTLD community is one of the vital components of how we do this. Right now we have Anne-Marie from .sc as one of the TCRs. But possibly other ccTLDs might like to be involved. We'd appreciate feedback on how to grow participation to support this effort.

Root Zone Management System Evolution

Just a few things going on with Root Zone management. Just a minor, relatively housekeeping thing. Recently we introduced new password constraints. In the past you could choose really simple passwords for RZMS. As of a few weeks ago, if you either reset your password or you add it to the system, you now need to provide a much more complex password.

We're at the start of the new fiscal year for ICANN, so we're in the process of prioritizing and planning out our roadmap for future improvements to the system. We're seeking feedback from you guys on

your experiences with the system as it stands today and your input to help us prioritize future work. We've had a lot of good suggestions. We have a lot of observations we made ourselves where we think things can be improved. I think the one piece that is missing in my mind is which of these are more important, and what's the burning issue that we should tackle first?

I'm going to run through some ideas and some plans that we have and any input we have on each of these is most important to any of you either today or later on, please pass it on.

On the technical and security side of evolving the system, firstly, we're looking at the technical checks that we do. The technical checks that we do were agreed around 2007 timeframe. We've received a lot of feedback primarily from the gTLD community. There's a lot of gTLD operators that didn't exist 12 months ago, so they've been exposed to how we do technical checks the first time. They provided a lot of constructive feedback on how they would like to see it evolve.

Some of the things we see, we have, for example, a test for what we call serial coherency. This test as technology progresses becomes a bit less useful. It gives a lot of false positives. So, we're looking at ways we can improve that. Network diversity checks.

But there's also new test to add. We've noticed some new weird DNSSEC configurations that it's pretty clear to us they're not intended to be that way. We then formally notice them and caught them and advised the applicant, but we don't automatically test for those kinds of conditions. There's a few new things we'd like to test for, so you as TLD

manager, if you've made a mistake in your configuration, you're aware of it, you can choose to proceed if you're sure that that's what you wanted to do. But if not, you at least know and you can take a look.

The second thing we want to work on – and I think this is an important piece of work – is an API. A couple of TLD managers from day one of implementing RZM asked for an API. For those who are not aware what an API is, it's a way of automatically talking to RZM directly with your software rather than going in via a web interface that you fill in.

The reason why an API has a high priority now is we're now seeing TLD managers with large portfolios of TLDs. They're managing 10 or 100 TLDs. So what an API enables is much more efficient processing of those requests. Rather than doing, for example, 100 different interactions, you can use an automated tool. It provides a lot more flexibility in how you lodge requests and manage requests.

A third thing we're looking at is proactive notification of issues. Right now, a lot of the stuff we do, like technical tests, we only do when you lodge a change request. So if you leave your IANA record alone for several years, we won't test anything in terms of your configuration.

One thought there is to – "Why don't we test on a regular basis in an automated fashion and notify you as our customer that if we notice anything has changed, we'll give you a notification via e-mail and you can look at it and work out whether it needs attention." So that would be sort of an optional service that you could select into.

Similarly, we see a lot of issues with DNSSEC signature expiry. We can send you some proactive notification if your signature is about to expire.

Another request we received on the security side is some TLD managers have said, "Well, for audit purposes, we want to know every time our staff have logged into the system." The notion that we could just keep an audit log of every time an account is used. You can go in and get a log of every time access was made in the last 12 months, something like that. That's something worth looking into. That's on the technical side.

On the administrative side, I think this is probably the most interesting part. I think one of the biggest gains we can get as we look to evolve our system is a new contact model. What I mean by that is that right now we have this notion of an initiative contact and a technical contact. This is a legacy from before ICANN even existed. Those that use InterNIC are familiar with – I think a lot of your WHOIS database models are based off the same concept. It was something ingrained from very early on the DNS.

The way we use the admin and tech contact right now has two completely separate prefaces. One is that these two contacts are listed in the public WHOIS. It's the contact point for your TLD. Secondly, we use them as authorizers for changes. So any time there's a change to a TLD, we expect both the administrative and technical contact to agree to the change.

Now, there's an inherent problem there which is that, firstly, the parties are allowed to authorize a change request of public information. So

arguably, there's some potential security implication there. But secondly, as a TLD manager in the modern environment, you probably want to list customer service contacts in the public WHOIS. But for something as fundamental as changing your TLD, you probably want someone senior, someone with authority to authorize change request. And so those two don't exactly reconcile.

So the idea of a new contact model is looking at potentially the implications of separating those two functions out, having publicly listed contacts and then having what I call authorizing contacts. And with that could come some flexibility. So you could have any number authorizing contacts.

Say for example, in your situation you had five different people you wanted to consent to any particular change, we could potentially set up something like that. So by un-wedding the WHOIS contacts from the authorizing contacts potentially gives us some gains in terms of flexibility of how you manage your entry in the Root Zone.

Another thing on the administrative level is contact normalization and sanitization. In short, there's a lack of consistency across some records in terms of the address format, the phone number format. We'd like to just simply tidy it up. So probably a mixture there of looking at some software solutions that do sort of address normalization, verifying with you guys individually on certain records whether they're accurate, just trying to bring some neatness to the database.

Another thing we run into regularly is people change their change request after they've submitted them. Right now it's actually not

possible to change request while it's in process. So if you notice a typo in your request in the middle of the processing, our only option is to withdraw it and go back to the beginning. So we would like a mechanism that we can do simple things like typo corrections and so on in the middle of a request. Obviously towards the end of implementation, once it's already going through for final implementation there will be some lock on that. But in the early stages of processing, we want the ability to tweak what you've asked for.

And then finally – and this is in line with the contact normalization – a lot TLD managers we only deal with every few years, and when the time comes a request actually needs to be made we find out an e-mail address doesn't work or some contact method doesn't work. So instituting more regular audits of e-mail function, some automated e-mail – perhaps we send out e-mail every three or six months, ask you to click on a link, verify that this e-mail address still works. If we don't get that, we'll do some more manual follow ups. Something like that.

Again, we're looking at making sure our contact database is up to date, accurate, and that allows us when the time comes if you need to make a change, then it should be very straightforward. I one of the biggest causes of delay we see in making change requests is that the authorizing parties we have on file are out of date.

Finally, the one problem that I don't have a good solution for – and there has been some discussion on some ccTLD mailing list about this recently – is how to improve authentication mechanisms for our system? Right now access to the Root Zone management system uses a username and password. We have a desire to implement stronger

authentication such as two-factor authentication, issuing you with one-time codes, that kind of thing.

In short, our customers on average do about one change request per year, which means that some do a lot more than that and a lot do a lot less than that. We find very regularly that when you come after a couple of years to do a change request that such-and-such a person no longer works here or that username and password you gave me two years ago, I forgot. I need a new one.

So the whole idea of increasing and strengthening authentication is actually you make it harder to log in but that kind of conflicts with the notion that a lot of our customers forget their credentials.

So this is kind of an open invitation for ideas. How can we strengthen the authentication mechanisms with that in mind? Can we lock down the system and make it stricter? How will that impact those that forget their credentials?

We can have a recovery process that's somewhat burdensome, that we establish everyone's identity before reissuing credentials, but what happens if there's an urgent change request that needs to be done today for a TLD to make sure it continues operation? Should we be holding up such a change request if we can establish that second factor with authentication? These are some of the questions we wrestle with.

Like I said, I don't have a magic solution here but I'd appreciate input on what's a good model to think about moving forward. Another facet to that is that a couple of TLD managers have asked us, "We don't trust e-mail authentication. It's risky. Can we switch that off for our TLD?" So

instead of sending confirmation links via e-mail for our TLD, they only want to be able to log in to the system and do it with the username and password. These are some of the conflicting objectives that we have. Again, I'd appreciate some thoughts on that.

That's really my presentation. Just on the last slide I didn't quite have it ready to share with you today. We are working on an infographic on how the Root Zone is managed. It's really not designed for anyone here at all. I think you're all familiar enough. It's everyone else that's talking about IANA right now that perhaps isn't familiar with how the Root Zone is managed to share some of the key concepts that are involved. So that's something that we're working on. We have to have a draft available for community review soon. So with that, thank you.

ANNE-MARIE EKLUND LÖWINDER: Thank you very much, Kim. I think that was excellent, a very interesting presentation. Any questions? Yup. [Don and Roelof].

[DON]: Thank you, Kim. A couple of comments and questions. When you talk about audit I think that's a very good idea. I would say, if you could, audit not just when somebody made a change but what change they made. That's just an old CIO [hat] issue.

I quite like your new contact model. When you said that when you do your evaluations of change requests submitted and you have a set criteria, I'd like to know how that criteria gets set and who sets it?

And then my last question, if you could talk about how IANA has gone to the length it has to support IDN in name servers and what you are doing and what you're not yet doing. Thank you.

KIM DAVIES: With respect to the first question, what are we checking for? I think broadly for root zone change request, there's two main areas of review. One is for consent. The consent model right now, like I said earlier, is essentially inherited from pre-ICANN times.

The other side is technical checks. Technical checks – I couldn't tell you where ICANN's original test came from exactly. I can tell you that when I started at ICANN in 2005, no one was particularly happy with them so that was actually sort of the impetus for the review that we did around 2006 of those technical checks. We had some meetings and we resulted in about a dozen technical checks that we've been doing ever since then. So that's really what's led us to what we do in that respect right now.

In terms of internationalization, we first implemented IDN TLDs six years ago now and we're mindful when we're implementing them that all of our systems needed to support IDNs, customers will be typing in IDNs and so on. We did a lot of system improvements at that time. We implemented a WHOIS server, for example, that has very good support for IDNs, for example.

But we have a lot of third-party systems inside ICANN, ticketing system and so on. Our ticketing system we commission the vendor to add IDN

support to it. It's an open source package so they've in turn – at least that is open source.

But some things, for example, our e-mail server is Microsoft Exchange. I'm pretty sure Microsoft Exchange to your point doesn't support internationalized e-mail addresses, so that's something we don't have support for right now. We try to be as responsive as we can to our customers' needs, so we try to monitor where we should focus our efforts. And yeah, our focus has been on accepting and using IDN domain labels, but as IDN support grows to other protocols we'll try and implement them as soon as we reasonably can.

ANNE-MARIE EKLUND LÖWINDER: Thank you. [Roelof?]

[ROELOF MEIJER]: Thank you, Kim. I just want to echo [Don], first of all. I think it would be a good thing to have [audit] trails. Secondly, I think stronger authentication mechanisms would be very desirable at least from my point of view.

I'm a bit lost with your [inaudible] urgent changes shouldn't be held back due to lost credentials, because I'm wondering how do you establish that the request is authentic if the requestor has lost his or her credentials?

But maybe a system would be that you start and you have an opt-out or something for those organizations that find two-factor too complicated they can opt out. That also leaves the risk with them instead of with

you, but I'm sure that we will prefer to have a more stronger authentication system than the present one. I'm sure that you remembered that when you introduced your new online system that we commented on the fact that passwords were sent to us in encrypted mails. So there's some room for improvement there I think. And I think also for IANA it will become more difficult to keep track because you'd be getting another 1300 customers.

KIM DAVIES: Thanks, [Roelof]. Yeah. I did race through the slide a little bit. I didn't want to exceed my 20 minutes, but a little more on that. The worst-case scenario is a hurricane goes through Caribbean island and we have to establish contact in some way that's very uncomfortable for them and we have to somehow establish that we're talking to the right person. Thankfully, personal relationships and so on has helped today, but we can't rely on that as a normal sort of business method that is trustworthy.

I think one thing that I skipped over is the second bullet point which is a complicating factor that's making it worse right now, which is that if you go back five or ten years, almost all the contacts that we had were people. Increasingly the contacts in our database are roles. And the roles they're just like CEO or customer service, and how do you authenticate someone who's authorized to speak for customer service particularly in a case where the normal methods of communication had broken down?

If it's a person and you have established that's the right name and the right person but they can provide identity documents through trusted party or whatever, send a scan of their passport, whatever the case may be. If it's a role, that is extremely difficult to do in a trustworthy way.

So part the contact discussion I think is about moving the pendulum back to individuals, not roles. And I understand the desire for roles is to have generic contacts in the WHOIS. Hopefully, when those two concepts is separated people will be more willing to nominate specific people in their organization to be authorizing contacts, and then we can have a better grasp on who are the people that are allowed to do authorizations.

ANNE-MARIE EKLUND LÖWINDER: Thank you very much. Any more questions? If no, let's thank Kim again. Thank you. So the next presentation is about ICANN dashboards and key performance indicator. I'd like to invite two presenters to give us more insight on what it's all about and what's really important. The presenters would like to hear your views. They really hope to receive some feedback from the audience. Therefore, please pay attention and give your feedback.

CAROLE CORNELL: Good afternoon. My name is Carole Cornell. I'm the Senior Director for Business Intelligence and Program Management at ICANN. Next to me is Aba Diakite and he is the Senior Manager for Business Intelligence for our department.

Today we're going to give you an overview of some of the business excellence/dashboard efforts in business intelligence we're doing. So we're going to give you an overview a little bit about the strategic structure we're using for building these dashboards. We're going to talk a little bit about process-driven culture, dashboard development and roadmap where we're headed right now, and then give you some samples and then if you have any feedback or questions, we'd love to hear them.

There's a meeting tomorrow morning at 8:30 to talk a little bit more in depth about this because we're just going to give you a high-level view today. So it's just to let you know if you'd like to know more about it, please come.

If any of you looked at the FY15 Operating Plan and Budget that's been posted recently, you see we've been using a similar organizational objectives kind of structure. So there's four organizational objectives here. There are 16 goals, and in FY15 there's [50] portfolios and you get the idea. So that operating structure is put together. This slide we put in to show you that we are tracking and we will give results going forward on how the cost of delivery fits within those goals and objectives.

I talked a little bit about a foundational piece of the structure. This shows how they're all connected both internally and externally. So the objectives, goals, portfolio, and projects are the foundation in which we took the strategic plan and the financial plan informs our yearly operating plan which informs how those budgets are developed and the project portfolios are all linked together, which informs how our performance does within our staff and then how that shows out as risk

management and executives. It's just to show there's a linkage of all that information.

Several people have wanted us to clarify a little bit about business intelligence. It is a set of methodologies and technologies that transform our data into a meaningful and useful set of information. We're hoping that our executive dashboards help make fact-based management decisions as well as be able to make sure that the key success factors have good key performance indicators that we share into a dashboard.

This is talking a little bit about the reporting and the dashboard and the fact that we're going to be collecting data and we put out dashboards, but there's also a reporting mechanism that's tied. And some people distinguish building a good dashboard, set of data with [raw data] into meaningful dashboards is [a key part], but [inaudible] reports to do.

I think this is important to share. This is to show you that we are at the operational level working on set of data and metrics every day. But we're going to roll it all up into meaningful dashboards that get presented based off of the objectives, goals, and plans. And this is just to show you that that is the process we're using.

I'm going to skip this. This is just a little bit of the cycle.

I'm going to talk a little bit about this. We have been developing and we already have the key success factors and we're working on the appropriate key performance indicators and pulling the data together that we do have. A lot of our data doesn't come from a central source. It's in different systems and it's one of the maturities we're working on.

But from a tool that you would see, is we're building a beta dashboard that we're going to be sharing in L.A. Right now, if you go on our site, there is a set of dashboards, but those are being archived and we are structuring it all with a common plan and format. This is the timeline we're using for that.

The goal for the initial beta will be to have one or two key success factors per goal or per portfolio which would show in a chart. And this just gives you a target and it also shows you how there's an accountability to the objective to the goal and the portfolio as to who manages those components.

I'm going to switch this over a little bit to Aba and let him talk about some of the specific examples because it gives you a chance to talk about the components.

ABA DIAKITE: Hello. The chart that you see in here is actually for the PMO office. It's about the project closure rate. And as a good dashboard and KPI, it got all the attributes in here. You can see that we're tracking on a monthly basis, the number of projects that we have. And in blue – let me probably zoom in here – in blue you can see the number of projects that are being completed. What you have in the far right, it's really the target that we gear into. So a part of our process like Carole explained before, what we have in there, that puts really the measurement into context. So you have the monthly measurement in here, and to put it into context in here, there is a target that we're trying to get into it.

CAROLE CORNELL: I would also share that the reason it says 85% is some projects carry over from year to year, so you would never get 100% as a target at the end.

ABA DIAKITE: This next chart is about the ICANN meeting participation per region. This is something that we've been using at ICANN that we cannot [inaudible]. That's why we have the ICANN meeting rotate between the various regions. Now that we have some analytics and we have some measurement, we put in the chart and it kind of allows us to really justify that measure and really be in a position to make fact-based decisions.

And a little bit when you look at the chart, you can see in here the first meeting, which is in Beijing, ICANN 46, you can see that the participation from Asia-Pacific is really the greatest in that chart. And by moving to the next meeting in Durban, you can see on the light blue, that's the participation from Africa who's dominating. So far in Buenos Aires, in the green, that's really participation for Latin-America.

And when you do an average of the last three meetings, then you can see that the participation is well-balanced among the various regions and [inaudible]. That's really the purpose of really the dashboard exercise. It's really to put into figures to put into metrics decisions that we are making. Let me go to the next one.

This is more charts that we put about the ICANN meeting, about the number of supported travelers. I'm going to skip those in here to kind of focus on the IANA chart. Earlier, Carole showed you the pyramid. She

showed you the pyramid about the different levels for the dashboard. At the highest level, you got the strategic level, and at the bottom, you have the operational level.

The approach that we have taken is really that multi-level dashboard. It's to provide the right information to the right person at the right time. What that means in here, the strategic level in here, you've got an aggregate depiction of the KPI here. For IANA, really, it's the key performance that we measure in here, it's the timeliness of how we process change requests in the root zone.

Here you have the target of 80% and the actual measurement [inaudible] 97%, that means it's a green light. The target has been met. So that's enough information to show at the highest level, the strategic level, for [oversight] purpose.

But if you're internal and for management purpose, you're going to need a little bit more data to be able to manage the operation itself. So that's here. We provide a [drill-down] approach so you can really actually track the individual requests and you can see where on the timeliness performance measurement where we're missing out. And you can see that there is a spike in here, and the operation manager can make the decision and actually can take action and see that the problem is not a systematic problem but it's probably a glitch with just one request. Can we go to the next chart?

The next chart, it's really the same approach. This is for delegation – re-delegation – for our generic TLDs and we're measuring the timeliness of the process. Target is 80%. This is 100% now. It's a green light.

And same approach. We [drill-down] in here to be able to see the individual requests. And that's really to show the highest level from the strategic overview for [oversight] purpose and in here for internal operation. I think that's the last slide. Yes, that's the last slide, so we can probably open for questions.

ANNE-MARIE EKLUND LÖWINDER: So thank you very much. Are there any questions? Yeah, Jorg?

JORG SCHWEIGER: The question would be could the tool show the allocation of staff to different projects?

ABA DIAKITE: Sure. The tool definitely will have the capability to show staff allocation, but as we mentioned, in the process, the key performance indicator needs to be aligned with specific objectives and goals. If that's the objective and that's the key success factor that we're trying to measure, then that's the chart that we'll build and present.

JORG SCHWEIGER: Could that [inaudible]?

ABA DIAKITE: Sure. If it's part of a key success factor for that project or for that objective [inaudible].

JORG SCHWEIGER: Actually I was just wondering because this doesn't seem to be included in the strategic and operational plan ICANN gave to the community, and I was wondering where we build up an additional 160 staff. And I was just wondering whether or not this would come out of your data, and obviously it would, so I would ask somebody else for that data. Thanks.

CAROLE CORNELL: Hi. I'll give you a little bit more in-depth answer to your question. When we were building the FY15 Operating Plan and Budget, we did estimate the resources per project per plan, and there is a spreadsheet of that as an allocation of hours, but it is a planned one, not actual. So it would be high level [and] we did that at the project level, but there is still some learning curve internally as to how detailed we want to get to those planned hours and some assumptions, so we have not put it in the operating plan at this time.

It is our goal going forward not necessarily in FY15, but our goal is going forward to keep building toward a more detailed project cost plan. So as that evolves, we would share that information.

ANNE-MARIE EKLUND LÖWINDER: Thank you. Matthew?

[MATTHEW]: Yes. Matthew [inaudible] from .fr. I'm here. Hi. Really it's good to see that progress that's been made across a period of time of several years

towards a more integrated view on KPIs. It's been a constant discussion within the SOP Working Group under Roelof's leadership. And I look forward to the time when those graphs get onto the operational plans and budget or strategies to highlight actual commitments by ICANN to hold a certain level of service and back the reasoning why it's actually an improvement compared to the current situation.

But what I understand from your presentation is that now, in the SOP, we can ask for this data. This point is well-taken. Thank you.

ANNE-MARIE EKLUND LÖWINDER: Thank you very much. Any more questions? Yes, I just want to note that if you have any questions to the room, you can ask them because we have nice cards – red for no, orange for so-so, and then green for a strong yes. So if you have any question to the room, you can see the temperature, so the overall feeling in the community. So do you have a question to the room? No? Okay, if not.

CAROLE CORNELL: To be honest, I didn't know we were going to do that. I don't have a specific one. I guess I would ask this. The goal that we're trying to do is base everything off of key performance indicators. Is your expectation that when you see a high summary level that that would be satisfying you, or would you want to always be able to drill down and how far would you expect to drill down to be?

So I guess if you're going to hold the card up, do you think the level of detail we're striving for with a community-based report is the right level?

ANNE-MARIE EKLUND LÖWINDER: Green for yes. Okay, maybe it's too complicated. So are you satisfied with what you heard today? Okay, it's going to be hard to measure.

CAROLE CORNELL: Here, I'll just put an example up. When we showed you the IANA report, we said the top set of box where it says "key performance indicators" which gives you a description of what we're trying to achieve for the metric, the target and whether it's actually met, and the color and direction. Is that the right level of information that you would like to see if you were looking for a key performance indicator chart for, let's say, IANA? Is that the right level or will you be expecting – so I'll say that's the first question.

ANNE-MARIE EKLUND LÖWINDER: Yes, at the right level, green.

CAROLE CORNELL: And then I'll say the level below it, which is a more granular one, would you want to see that level of [inaudible] or would you think that the bottom one is too much level of detail for you and you'd really just be comfortable showing the top level?

ANNE-MARIE EKLUND LÖWINDER: Thank you very much. Maybe next time we'll do a more interactive session. Thank you. Let's thank our presenters.

[applause]

Next presenter, we have a presentation about Web Accessibility. That's the new ICANN At-Large Accessibility Taskforce is going to present about objectives and actions to build a culture of accessibility within the ICANN community. So Gunela will have presentation on the objectives of this initiative. So the floor is yours.

GUNELA ASTBRINK: Good afternoon, everyone. First of all, I'd like to thank very much the ccNSO to give me the opportunity to speak with you this afternoon. My name is Gunela Astbrink, and I'm from, first of all, ISOC Australia and the Asia-Pacific Regional At-Large. And within At-Large, there's recently formed an At-Large Accessibility Taskforce, an Ad-Hoc Accessibility Taskforce. I'm speaking with you today about web accessibility, generally.

So what is web accessibility? It is designing websites so that more people, including people with disability, can use online resources. And there are well-established W3C web content accessibility guidelines. They're called WCAG 2.0 for short.

WCAG 2.0 is mandated by governments for public websites. There are various levels of WCAG 2.0 guidelines, and usually it's level AA. It goes up to level AAA. Level AA is usually what is mandated by governments. I

should say by some governments that enable government websites to be accessible for as many people in the community as possible.

Now, why is this important? Well, actually, there's one billion people with disability globally. This is according to the World Health Organization. We're not talking about a small number of people. So there really is a demand for accessible websites so that everyone has the opportunity to make use of online resources.

Actually, web accessibility is an advantage to people on low bandwidth, because for example, if there's a lot of images and a person wants to turn off images, if a website is designed with accessibility in mind, there are adequate descriptions of the images, especially if there are links on the images.

There's also a correlation with higher search engine optimization. We all want to ensure that our websites are high when we do searches, so there are a number of benefits.

The UN Declaration, the UN Convention on the Rights of Persons with Disabilities, has been ratified by over 100 countries. One of the articles in this UN convention includes accessibility to ICT and that means, again, accessibility to websites. And that's Article 9 in that UN Convention.

I just want to note ausRegistry in Australia, the ausRegistry approach. It supports and creates awareness of web accessibility, and it has done this as a first exercise. A news article entitled "Why Website Accessibility Makes Business Sense." So we're not only talking about corporate social responsibility, human rights, it's a good thing to do.

There actually is a business case for this, and that is explained in that particular blog which you will find a link to.

Now, I mentioned to start off with that there is an At-Large Accessibility Taskforce. It is brand new. We had our first meeting at ICANN 49 in Singapore, and you will find there a link to the details of that meeting, which included a set of objectives and actions that were presented and supported by the people attending the taskforce. And importantly, we have the Chair of that Accessibility Taskforce in the room, Cheryl Langdon-Orr.

Now, the objectives that are presented at the At-Large Accessibility Taskforce comprise three main areas. One is building a culture of accessibility within ICANN, and that's incorporating this idea of inclusion and inclusiveness in ICANN policies and processes. And under each of these high-level objectives are a number of actions. I'm not going to go into those, because we're concentrating on web accessibility.

The second objective is increasing web accessibility, which is what we're talking about here.

The third one is ensuring minimal barriers to participation and engagement with ICANN processes and practices. So ensuring that we all can participate on an equal basis as much as possible within the ICANN community.

So looking in more detail on objective two, increasing web accessibility, these are the actions that the taskforce are considering working on.

The first one is that ICANN websites meeting internationally recognized W3C web content accessibility guidelines, WCAG Version 2 Level AA, which I mentioned before. And this includes captioning of videos.

We often think about web accessibility in terms of blind and vision-impaired people who need screen reading software with usually voice output to be able to navigate and obtain information from websites. That's very important, but there are many other groups who benefit from accessibility and these particular guidelines and that includes people with hearing impairment and who are deaf. So therefore, captioning of videos is very important.

The second action listed here is the development of ICANN policy on web accessibility, and hopefully this is something that we can work on in future.

The third action is encouragement of ccTLDs to develop a best practice guide on web accessibility, and that is one of the reasons why I'm happy to be able to speak to you today.

The fourth is encouragement of registries to use a best practice guide in relation to registrars. In particular, to alert registrants to use WCAG Version 2 when developing websites.

So that's really the guts of it, that it's this chain of raising awareness and assisting registrars and alerting registrants to web accessibility.

An example of best practice, the NETmundial website. We know that cgi.br and the local Brazilian W3 office were instrumental in designing the NETmundial website. This was designed right from the start using

W3C web content accessibility guidelines. There was no need to retrofit, which is often a lot more complicated. It was designed to meet those guidelines and to be accessible. And not only accessible, but attractive and easy to use, but it still was fully-featured.

And I'm sure many of you would have gone through that website, seen the draft content before the NETmundial meeting and you would have noted there were opportunities to comment online about various parts of a document. Well, that was all accessible. And so it indicates that these best practices are there and we can all make use of them.

I just want to draw your attention to NETmundial Multi-Stakeholder Statement. We have talked about this statement in many meetings since the NETmundial meeting. One of the principles under human rights principles in the document states "accessibility, persons with disabilities should enjoy full access to online resources, promote the design development, production and distribution of accessible information, technologies and systems on the Internet." So there is an example of best practice already there for us.

Now, what's the relevance of this to the ccNSO? Well, the ccNSO is ideally placed to facilitate voluntary best practice on web accessibility with ccTLD managers and it can consider adapting a Web Accessibility Awareness Guide for use by ccTLDs.

For example, the At-Large Web Accessibility Guide, there's a link to it here and I have a print-out with me if anyone is interested in that. This is just one way of presenting the information. There might be other ways that the ccNSO would be interested in doing that.

And also, the ccNSO may wish to encourage registries to use this type of best practice guide or something similar in relation to registrars. In particular, to alert registrants to use WCAG Version 2 when developing websites.

I just thought I'd mention going through the ccNSO website, there are guidelines for presenters at ccNSO meetings and talk about presenting clear slides, using Sans Serif, script, not to have too much text on each slide. Very useful information. That type of information about presentations is not only useful in this context, but it's useful as an example of best practice and inclusive design, which means that people with disabilities would more easily be able to access slides and these types of presentations. So I can see this type of best practice already happening.

So what are the next steps? Well, really, this is up to the ccNSO community. A couple of maybe early suggestions is considering future contact with the At-Large Accessibility Taskforce. Cheryl and I would be very happy to discuss any possible next steps with the ccNSO. So thank you again for this opportunity to speak with you.

ANNE-MARIE EKLUND LÖWINDER: Thank you very much.

[applause]

So are there any questions or any suggestions? Eberhard?

EBERHARD LISEE: Given my profession, I have a lot of insight into some of these matters. I wonder, you're aware of what ccNSO does and doesn't do or are you willing to become the issue manager on a policy development process as far as the ccNSO is concerned?

GUNELA ASTBRINK: I'm happy to assist in any way. I realize that ccNSO has a particular mandate. I noted that best practice in working with ccTLD managers was listed on the website. I'm happy to work with you, and so is the Accessibility Taskforce I believe, Cheryl.

ANNE-MARIE EKLUND LÖWINDER: Cheryl, any comments? No, okay. Thank you very much. Anymore questions, comments, from the audience? If not, then thank you very much for your presentation.

And now the exciting moment we've all been waiting for. Never before we had a presentation on Framework of Interpretation Working Group. Very good. We can't wait. [inaudible]. We'll brief you later. Keith, the floor is yours.

KEITH DAVIDSON: Gosh, what a mess of [inaudible] has stayed behind to attend this session. I can see it's of top importance. I do apologize for being between you and the bar, so I'll keep this fairly brief.

The FOI Working Group, for those who are not familiar with that that is, it is the Framework of Interpretation Working Group and its task has

been to develop a framework of interpretation of the policies and guidelines that exist for the delegation and re-delegation of ccTLDs.

It has been meeting over three years and it's come fairly matched to the end of its wick. I think I promised you all at ICANN Singapore that we would be finished with the framework and have it here for your approval. However, that hasn't come to fruition. There were a couple of small issues. Sorry, they're not small issues, but there are a couple of editing issues that arose that are of particular importance.

I think the thing to note is that this working group has been seeking to provide really concise clarification of existing policies and guidelines and we found a couple of points of ambiguity or lack of clarity and seeking to improve the wording so that there will be no such possibility of misinterpretation.

The aspiration of the framework of interpretation is to provide it as an approved document from the ccNSO and the GAC to the ICANN Board, and that the ICANN Board will use greater color and depth from that framework to make its decisions over delegations and re-delegations. Our hope is that their decisions will be more transparent and more predictable.

We reported to the Board this morning as part of the ccNSO session with the ICANN Board. There was strong support for the framework some Steve Crocker, from Mike Silber, and Chris Disspain and other Board members and they were going to take that message to the GAC and reinforce the Board's hope that the GAC will seek to approve the framework in short time.

We also reported to the GAC this afternoon, and the only difference between the ICANN Board and the GAC [inaudible] was that we also recorded our [inaudible] [Frank March] from New Zealand government on the GAC who has retired from his role in government and has been lead from the GAC on the working group on the way through.

The working group is meeting here at 9:00 a.m. to midday local time in Cadogan room. It's an open meeting if anyone wants to come along. I think at that meeting we will [inaudible] the final bits of text. In fact, I'm quite keen to lock the doors and not let anybody out until we have 100% unanimous agreement on the framework.

That does mean, though, that there is a process for members coming up. Some sort of vote of approval from the ccNSO membership that will probably need to be conducted on list in some form intercessionally. What we'd really love to do is get that done, get the Framework of Interpretation to the GAC so they can translate it into their languages and we can have any intercessional discussion with the GAC so that the GAC and the ccNSO can walk together to the ICANN Board in Los Angeles in October with the final framework.

I think, just given the quantum of work that stands now in front of the ccNSO and other constituencies in terms of the NTIA transition, the accountability framework and so on, it would be really nice to put this piece of work to bed, and we are at that very final stage. So please be aware, be interested, and be ready to make your comments and signify your approval.

With that, that's my report.

ANNE-MARIE EKLUND LÖWINDER: Thank you very much.

[applause]

Are there any questions? Nothing to add? Thank you very much. Thank you, and I'd like to close ccNSO meeting for today. I hope to see you tomorrow. We start at 9:00 with a very interesting session. Not really interesting session. For the first time, we'll have registries versus registrars meeting.

Even though we finished for today our official part, we still have unofficial socializing, and that's, as you can see now, on the screen. The ccNSO cocktail, it's walking distance, around 15 minutes of walk. If you prefer to travel in packs, you can come down at quarter to 7:00 and there will be an organized walking to the place. But of course, you can walk all by yourself. It starts at 7:00, but you don't have to be at the beginning. You can join any moment.

And of course it's possible, thanks to our generous sponsors. I really would like to thank .au, .cn, .kr, .ml, .uk, .br, .no, and .ni for making this cocktail possible. So thank you very much. See you tonight, and tomorrow of course. Tomorrow, yes.

[applause]

[END OF TRANSCRIPTION]