PRAGUE – FY 13 SSR Framework Open Consultation
Wednesday, June 27, 2012 – 08:00 to 09:00
ICANN - Prague, Czech Republic

Male: We're going to get started in just a minute, we're in the process of loading up the slides on the Adobe Note and we'll get started very soon

Male: Is this recorded?

Male: This is recording, so for the purposes of recording, we have Patrick Jones from the Security Team, Jeff Moss and John Crain also with the Security Team.

Patrick Jones: So for those that are remote and we do have a couple remote participants, while we're loading the slides and I'm going to turn it over to Jeff to introduce himself and we'll talk about the team and we'll talk about why we have done this consultation or initiated this effort.

The Security Team is one of the few teams that publish an annual framework of its programs and activities. We did this last year at the Singapore meeting and provided an update on our FY12 activities. In the meantime there's been a Security, Stability and Resiliency Review Team effort under the Affirmation of Commitments and that review team completed its final report right before the Prague meeting.

The Security Team has also recently posted its FY 13 SSR framework which we're in the process of loading onto the Adobe Connect. And in addition to that we have a document that is a draft statement of ICANN's role in Security, Stability and Resiliency. And those two documents are out for public comment right now. So we're going to use this time for those remote and also for the recording, for our own inclusion in the comment summary to have some hopefully interactive dialogue with those remote, because there's four people in this big room. And it's also early but that was the time that was also available. So with that I'll turn it over to Jeff.

Jeff Moss: So I'll just say hello, I'm Jeff Moss the CSO of ICANN and as Patrick mentioned the Security Team put out its budget where what we're trying to do with the budget is be more and more detailed with the budget each time, I know some of the comments from the SSR Team was that it's big and opaque and a lot of things go in the Security Team Budget, so we've been trying to get a more detailed breakdown that we can share with the community. And so this is the next step. And in the future we hopefully get as transparent as we can possibly get.

Bill Manning: Jeff?

Jeff Moss: Yes, question from Bill.

Bill Manning: I'm assuming that we're going to be sort of interactive here?

Jeff Moss: Yes, I hope so with four people. We'll count ourselves.

Bill Manning: In doing security work and particularly budgeting, occasionally there's a box that says we don't really – this is for the outside guys. So this is Bill Manning, and my question to Jeff is having served on this Security, Stability and Resiliency Review Team, one of the questions that we discussed or talked about had to do with occasionally the need for having opaque budget. And while openness and transparency is highly desirable and particularly in ICANN's case and particularly given the rapid changing nature and growth of the security section that you're responsible for, do you see the need for an opaque box for budgeting?

Jeff Moss: Yes. There will always be an opaque box, but my goal is to make it as small and as necessary as possible so it doesn't become just sort of a catch all for things. So there are certain projects and certain things that we just don't want to share.

Bill Manning: Thank you.

Jeff Moss: You can probably guess what some of them are.

Bill Manning: Oh, I don't want to guess, I have a vivid imagination, so I don't really want to guess. But going forward I mean that seems as you develop a budget, you can sort of cut that piece out relatively easily.

Jeff Moss: Right. Did you guys get the Adobe?

Male: Yes.

Jeff Moss: Actually it looks good, we're not going to project it on the screen, but the Adobe Connect link is working properly and the slides online work.

So from the FY12 version to FY13, we have updated the base terminology that we use, so from a starting point and some of these – this is an update, the resiliency definition has been I think –

[background conversation]

Jeff Moss: Yes, apologies for the logistical challenges, for those remote, here we go. It's going to look worse for those in the room than those remote. So this comes from the draft Role and Remit Statement which is based on recommendation one of the SSR Review Team. We've taken the

initiative even though the report has been provided to the Board and it still needs to go through that process to publish the draft statement.

This statement includes some base terminology and we've tried to come with a way to initiate the community discussion around what it means to coordinate what it means, what's ICANN's tactical mission, it will at least start to have some consultation around the role of ICANN and also the community and SSR for the unique identifiers.

Go to the next slide. Our annual framework is divided into two sections; Part A focuses on ICANN's role in the ecosystem and try to divide ICANN'S role into those things that are operational, so ICANN's manage of L-root, DNS operations, the DNSSEC key signing infrastructure, management of the IANA functions and also new gTLD operations.

The second layer would be ICANN's involvement as a coordinator, collaborator and facilitator with the global community.

And then the third area would be ICANN's engagement with others in the ecosystem.

So the next area of what we've tried to put some clarity around is ICANN's technical mission. This can be interactive for those in the room and also those remote. In the chat – okay so if anyone remote has questions please post them in the chat and we can answer your questions that you have.

Go to the next slide. With the framework and also with our Role and Remit Statement we've tried to provide some clarity around those things that ICANN does and does not do in SSR. And this has remained fairly consistent since the 2009 framework; we tried to state very clearly

that ICANN does not play a role in policing the internet or operationally combatting criminal behavior. ICANN does engage with and provide an opportunity for law enforcement to participate within the ICANN community. One of the things that has become more apparent over the last several years is that the law enforcement and operational security community do not neatly fit within ICANN's constituency and stakeholder group structures. So at this meeting and at other meetings, we've provided an opportunity for that community to meet and reach out to other advisory committees and stakeholder groups and that's just part of the security team's role in serving as a bridge between the technical community, law enforcement, the registry operators, ISPs and others.

Next slide. We're going to go fairly quickly through these next set of slides, that way we can get to the part that is about the team and what our main areas of emphasis are. Next slide.

I guess before we get into the introduction of the team and our core project areas, the questions that we're projecting online go into the Role and Remit Statement that is out for public comment. Some of these – yes, Patrick?

Patrick Jones: Can you go back one slide? When you have text like ICANN cannot unilaterally – is it not the risk that that is creating more question than answering them? Because then people might then ask okay so can you please explain when you suspend the domain names.

[background conversation]

Jeff Moss: Dave Piscitello is joining us in the front, also on the security team. In some scenarios law enforcement will actually subpoena ICANN. Often it's because they don't quite understand that we can't do this directly. And in the case where the order is a sealed order, you're generally not supposed to – you are actually prohibited from going and telling any other party about the seizure. So that means ICANN can't go to the registry, unless they go back to law enforcement and the court and say you've prohibited us from talking to the party that we much talk to in order to suspend the domain. So in that case we are actually part of the chain of execution and that's why – we don't unilaterally suspend domains but in some case we're actually parties to the suit.

John Crain: This slide set is to sort of inform people when there are dealing was about things that we really can't do. There is a misconception out there that ICANN can do this and there's other documents including something that they put out about how people should get domains suspended, but the important thing is it's not ours.

Patrick Jones: No, I was more thinking about the actual words that were used on the slides like how clear are those words for non-English speaking people in other parts of the world, not living in US (inaudible) more than asking what the actual process is. Thank you.

Patrick Jones: Instead of unilaterally, you would like directly or something?

Male: I just thought that I could raise a warning sign that people start thinking when they see that.

John Crain: I think that's a fair comment. We've not had any negative feedback on it yet, but yes, we will keep an eye on that.

Patrick Jones: Good, so I think the important thing here which I also heard you explain is that the key here is "cannot" not "unilaterally". Thank you.

Jeff Moss: So with our draft statement on Role and Remit, we have posted some questions for the community. Some of these questions are intentionally quite open-ended and hoping to generate some dialogue.

Patrick Jones: And since the comment period is still open, we're hoping to draw some online comments, we want people to think about this and take some time and send your comments in, because this is really going to inform the debate not just within the Security Team, but within ICANN and the various supporting organizations. We're finding that it's confusing to people not familiar with ICANN and foreign governments when talking

and thinking about what ICANN can and can't do that it's important that we have a clear statement of our role in coordination. So if anybody in the room wants to kick off a conversation on this, we would appreciate it; if not.

Jeff Moss: So we've noticed that there's been an evolution in the environment since we posted the FY12 framework and in the development of the FY13 is that there's been continued option of DNSSEC by TLD operators. We're now up to I think it's 87 or 88 top level domains have signed their zones. And over the last year we've had the expiration of the free pool and IPv4 address space, and we just did world IPv6 day, was that in early June? There's been a continued growth in the number of IDN ccTLDs and now that the new gTLD process has launched in addition to that, there's been quite a bit of international events, legislation and government intervention efforts that have all occurred since we've published the FY12 framework, next slide.

We thought this was useful, especially for the community to see that over the last year there have been a number of entities and governments that have published their principles for internet so we have links here, we thought it was useful that this just provides some guidance for the community as you consider security, stability and resiliency, there is significant discussion around the multi stakeholder model and internet governance and these are some good documents to review in the context of events that are coming up later this year.

As I mentioned, our team is quite unique because we've gone through the process of publishing an annual framework, so this link, page of links

provides the background of our previous plans and frameworks that have been acknowledged by the ICANN Board. So our timing is that we're in the process, we did an advanced preview with SSAC earlier this year. We've also provided an opportunity for improvement to this draft and now that we're in the consultation process, through the Prague meeting, I believe the comment period ends in early August and that we're continuing to reach out that we've also – our fiscal year begins in the 1st of July so we'll be already in the middle of FY13 and needing to start to progress on our programs and activities.

So as I mentioned our annual framework is divided into two parts; Part B focuses on the things that are key programs and initiative for the coming fiscal year, and in response to the SSRT recommendations and also our conversations with the community, we added in a new module this year at the very end that provides a status update on those things that we said we would do in our previous FY12 plan and shows how some of those projects and initiatives were executed on during the year.

Do you want to talk about how team fits in with the other teams in the organization and some of the –

Male: So internally, the Security Team supports overall operations within ICANN from supporting the legal department, supporting HR, supporting our own IT infrastructure systems. And so when people think of the ICANN security, sometimes they think of us purely as external engaging with SSAC or RSAC but two key members basically focus full time on the internal activities within ICANN just kind of keeping our own house in order, and we provide both sort of risk and security comment for any

questions that come up from any executives in other teams – okay, you want me to go through some of these.

And so what we're doing is we're providing as you see on the list, we're infusing sort of security resiliency as a core value within ICANN, there is four pillars and security is one of them. In the strategic plan and as I mentioned we're a standalone department with a pretty good budget and as we find through activities such as bringing the new gTLD program online, the security team is heavily involved in testing internal programs and identifying issues and that has raised the profile of the security team within the company. And so we're being viewed more as an essential element for these future programs and projects.

So as you've guessed previously some of the team members, Patrick more specifically spent a lot of time coordinating for the SSR review that just completed and will probably still be engaged in the next couple of months with some post SSR reporting. We've spent a lot of time externally focused also with global security engagement, awareness, thought leadership, there's areas – do we have the collaborator influencer slide coming up? Okay, so I won't go into that. Just go to that one… Oh, no, we don't have that one.

[background conversation]

Male: John, you did quite a bit of training within the ccTLD community and also some of the operators, do you want to talk about some of the

training that we do as a team that gets to providing education and awareness?

John Crain: So we do actually spend quite some resources on time working in cooperation with others in the community. Our focus is really on the identifier system, so we tend to spend a lot of time working with ccTLD organizations. We're also working closely with the Commonwealth Cybercrime Initiative, once again to expand the capabilities of mainly ccTLDs and people in the identifier industry.

Typically these trainings are on an asked-for basis, you know somebody will come to us and say our organization is a grouping of operators in this industry, and could you come and talk to us about X, Y or Z. Generally, X, Y and Z tends to be about either security practices, issues around operating a stable infrastructure, and sometimes just what does ICANN do kind of outreach. We published where we're going to be on our security website, www.ICANN.org/en/security and you'll also see if you look at for example any of the TLD organizations, you'll see that trainings also mention us.

And if people have input on how we can hone this or if we're not reaching the right audience or the right topics, then please feel free to come forward either to myself or any of those organizations.

Patrick Jones: So we're projecting a slide that describes who's on the team, and to start with we added Jeff Moss and April last year, so now you've had over a year on staff at ICANN.

Jeff Moss: I think I'm just starting to understand how this organization works.

John Crain: Good, when you figure it out, could you tell us?

Patrick Jones: So we also have Geoff Bickers who is not at this meeting, but is heavily involved with our meeting security as well as our internal and information security efforts. John, so you want to talk a bit about some of the things that you do?

John Crain: Well, I think I just a little bit about it, but I work a lot in the outreach area, trainings, trying to get information inside as well obviously when you're out talking to people, you hope it's a two-way conversation, so I also try and bring input from outside of what people are expecting of us.

[background conversation]

John Crain: Yes, another thing you'll see one of the things I've been an advocate of is not flying the flag too much, so when we are out there giving trainings, you won't see them advertising us in ICANN training, it will be a LAC TLD training, we just did a training at [CarribNOG] but we're not trained to be the world's training expert here, we're just trying to be a

resource. So you may not actually sometimes be aware that we're doing these programs, because although it's in our budget and we consider it part of our mandate, and we're very open about the fact we're not there, there's not a big advertising campaign or anything. So sometimes we may already be doing trainings in your area and you don't even realize it. As long as it's good training, that's all that should matter to you, don't worry about who's doing it.

Patrick Jones: So we also have as part of the team and available resource Whitfield Diffie as VP for Information Security and Cryptography and started as an adviser to the CEO. I'm Senior Director of Security and I kind of keep the team coordinated and manage our budget and also coordinate with our external efforts, so that has primary has been our SR framework and being available as a resource for the different review teams also what do you think, being annoying?

John Crain: And also being a whipping boy.

Patrick Jones: Okay, we also have in the room Dave Piscitello who was previously a few years ago on policy staff and then became sort of a hybrid policy security person, now we're really to have Dave full time as part of the security team and also with his depth of knowledge in the policy area. So you don't have to stay in the audience, you can come up to the stage if you want.

Someone who is not here but has become a really fantastic resource for us has been Sean Powell and we owe him major thanks for his efforts in information security and working on our networks and providing us with better visibility.

And not least but Rick Lamb who is Senior Program Manager for the DNSSEC efforts, the key signing infrastructure, we just did a key ceremony in Culpepper, I think about a month ago, and he's continuing to spread the message on DNSSEC and encourage the option and lead training.

Jeff Moss: Rick maintains the page under security where we track which registrars support DNSSEC, DS key entries by end users, that's one of the pages that Rick maintains as his overall effort to try to gain visibility and awareness around DNSSEC.

Patrick Jones: Dave, do you want to talk a bit about some of the – in particular the thought leadership area, we posted a paper before the Costa Rican meeting on domain seizures and take-downs and some of the things that you do.

Dave Piscitello: Part of what I've done for most of my career is try to raise awareness on dot security issues, step back and take a look at systemic problems and see whether there is some you know relatively straight forward documentation that could actually simplify and make processing or

solving a problem much easier just because there's a document for people to actually converge on.

And when I came to the SSAC and actually after I came to the Security Team, I've sort of continued to spend more time in global outreach than actually in ICANN core policy and largely because there is so much going on in the security community and law enforcement community that touches the domain name system and registration services that needs to have some sort of bridge and liaison.

There is such different language, such different appreciation of time and urgency in some cases, different needs of law enforcement versus needs of business and competition. So an example of that kind of activity was a paper that Patrick's referring to that kind of steps back and doesn't take a posture on whether a domain name seizure is an appropriate thing to do in every case, it doesn't make a judgment, it simply says there will be a time when somebody will serve you an order as a registry, or somebody will serve you an order as an registrar, and you're going to comply because that's just what you do. You know most people prefer to comply than to go sit in jail.

And so if you're going to comply, you probably want to have the best information, so complying is not a nightmare for you. And so what we did, we went around and we talked to the security and operations people, we talk to law enforcement, we talked to registries and registrars, and we came up with a paper that said here is the documentation, and here is the way you could present it, so that we could process your court order in the most expeditious fashion.

And John and I actually did a little bit of a road tour with the paper in London when we were there last, and we happened to have an opportunity meet with a number of people from European Trade Offices and Consumer Rights' Offices who were visiting of Office of Air Trade in the UK at the time. And the paper was exceptionally well received, and they said if only we had had this a year ago, but now they have it and moving forward that builds a really positive relationship, not only for ICANN, but for the registries and registrars, because we all actually want to solve the problem. If we can set our differences aside and realize we don't want crime, and this is just one of the ways that we do that.

Patrick Jones: So as you've guessed, Dave is one of the primary standard bearers in our thought leadership component of one of the four areas that the security team operates in, in an influence area.

Dave Piscitello: So there's actually one other point.

Patrick Jones: One other point?

Dave Piscitello: You know one of the other things that we are doing, John and Patrick and I before Jeff came on, had started to realize the value of relationships with some of the operational and security communities. So we've begun a much more closer relationship with the anti-phishing

working group as an example. And in April when they were here in Prague we sponsored it at a modest level.

In October we are going to be one of the platen sponsors and we're hosting our DNS Security, Stability and Resiliency Symposium in conjunction with their October meeting which gives us a really good opportunity to bring people from the DNS expert community into the same room with the people who are fighting a lot of the – most significant cybercrime and will be present at that meeting and hopefully they'll stay a day and carry over and work with us.

So I'm excited about that because I've been crossing these two communities for about seven years, and I think that this is only going to have a positive impact on our community. If there are questions and…

Male: There's a microphone up here.

Male: Pass it back.

Marilyn Cade: My name is Marilyn Cade. I want to say how much I appreciate the fact that you're doing this briefing, and I know sometimes I think I particularly was affected by an interpretation that the Chair of ICANN made that because people were not in the room during the presentation that no one was listening. And I Chair the Business Constituency and briefings like this which are then available to be returned to and shared at other times to the broader business

community are really, really helpful. So I just want to express my appreciation.

I'd also like to comment about how impressive the willingness and availability of the team to interact and be subtle about the face of ICANN but effective about the presence of ICANN. I think you're really taking the right approach. And I see and hear very good things when I encounter – in particular people from developing countries who are having the opportunity to interact. So now I want more.

John Crain: Good. Please put that in writing on the comments that will…

Marilyn Cade: I will but I have a specific request I'd like to make and I'd like you to think about. The Business Constituency publishes a newsletter now for each of the meetings. And we will do an eight-page version for Toronto and I'd really like to sit down, and perhaps Patrick we could do this while we're here and think about whether we could do something in the newsletter that is pitched to business users about the work that ICANN is doing. I think that might be very helpful for us, in particular with the number of brands that are going to be coming into the new gTLD program; I think we're going to have the opportunity to reach into some of the technical sides. And particularly Dave topics like domain name fraud and abuse, and take down and other things. They may be looking at a different of the equation. Many of them as you know are very active in the anti-phishing working group. So that's one request I'd to think about and I think we'd be very interested in trying to do that and

make what you're doing more visible, but customize the story for business users.

And then secondly I think – I started this conversation yesterday when Patrick and Jeff came to meet with the Business Constituency. I think we need to as the community look more carefully at the scope of the awareness and information initiative that ICANN can support to reach perhaps a bit more broadly into the internet ecosystem. And we could perhaps take that up off line a bit.

Dave Piscitello: So for the first one, if you get the nod from Jeff and Patrick you know I've been freelance writing or self-publishing for 30 years, I just need topic, word count, deadline. So that's how I made my livelihood before I came to ICANN.

For the second, we actually are doing some things that we didn't talk directly about, for example, I've been invited the National Cyber Security Education Council. Jeff is involved in a similar effort inside the beltway. And I work with Lance Spitzner in the STH community. And with the stop and connect initiative to try to raise security awareness and if you go to their site, you'll see that many of the articles that I've written at my site are linked and we do a lot of cross Tweeting to try to raise that awareness and much of my writing about domain names is here is how you protect yourself from these dangers. Writing something like that for the business community raises up a little bit of the business emphasis but it's very much the same signal that we are trying to amplify everywhere.

If there are some specific things or specific places in the business community where we can go and we can talk about some of the issues without getting sort of sucked in to the piracy, privacy right, you know because frankly you know me, I'm not aligned there, but if there is like a generic set of topics I think any of us are willing to do that.

Marilyn Cade: Although the Business Constituency has members who are trademark protection and is a very high priority to business users, but the primary focus we take in the Business Constituency is the concern that comes from misuse and abuse of domain names, not that we don't have a sister constituency who has members who are very active in broader areas. But I think Dave for this particular purpose for all of you what we would like to do is focus on sort of what to do and how to respond and why you should get involved in ICANN from the business problem that is caused by misuse and abuse.

Dave Piscitello: There's another question in the room.

Alejandro Pissanty: Good morning, my name is Alejandro Pissanty. I congratulate you the ICANN SSR Team for putting forward new documents for consultation, in particular for putting the SSR framework in this new form.

I pick up on Marilyn's point specifically for this intervention which is one of the many findings that are behind the recommendations in the Stability, Security and Resilience review which we have just delivered is

that all three considerations, Security, Stability and Resilience are a systemic system-wide consideration and are systemic from a systems point of view, consideration. And I think it's very useful to think a bit directionally where Marilyn has already spoken for ICANN to find in the Business Constituency people who will convey not only the security messages to say that you need specifically about managing domain name abuse, about reacting to domain name abuse, about preventing and so forth, but also to carry the message that ICANN is doing these things and people come back to our credible ICANN that's contributing positively to this mission in fields where it's key.

And I will add this to the obvious, which is say the English speaking larger business community as well as the large community out there which still perceives ICANN unfairly or unduly or with too much weight as an American corporation that's in charge of the internet, where you can really limit the perception to the actual mission of ICANN and then improve the perception of ICANN as a positive force. I think that's – Dave as offer to write the Business Constituency and many others have lots of people to write and venues where they know their audience is and how to tune the message for them, and this has to be then a bi-directional large cooperative.

Marilyn Cade: So can I add one more request. Have you so far taken a look at participating in the national and regional IGFs initiatives as speakers?

John Crain: Yes, we do get invites for that. Obviously generically there is a lot of policy discussion and ICANN stuff there, but we also – we're a resource for the community, the IGF is part of that community, so if we get asked and obviously budget constraints and all that stuff, the answer is yes. Okay. That's good.

And on the issue of how we do the outreach, et cetera, it is one of things that we struggle a little bit with is making sure that we package these materials correctly including the issue of having them in other languages, et cetera, and also the format et cetera that we do to make them more accessible and so also the people can share them. You know we don't have to give these discussions or these trainings if we provide the materials in the best way.

And pretty much anything that we provide in training we automatically make that an open source of public comments so that anybody can use and try to do a bit of training of the trainer as well.

Patrick Jones: Also Marilyn, based on work that Rod had done participating at the World Economic Forum in Davos last year, ICANN was asked to participate recently in the World Economic Forum they have sort of their own security stability section, cyber resiliency. And so I recent participated in the World Economic Forum in Southeast Asia and we were going to be asked to help provide comment on their five sectors of risk analysis. And I think this is important because I think your group in particular with a growing number of people in the new G program, we're going to see a lot more business people that are business people coming to ICANN.

And so we view participating with groups like the World Economic Forum as a very valuable new group that we need to be visible and active with, so that's something we're planning to continue our involvement.

Dave Piscitello: Before we get off the IGF train, John has done some work, but also SSAC has done quite a bit annually with IGF, so I wanted to make certain that Patrick could actually explain our process and how the SSAC actually does IGF, or the gentleman to your left can handle it.

Alejandro Pissanty: I hand over to Jim.

Jeff Moss: Yes, for the past three years and we're doing it again this year what SSAC has done, is we've looked back at the work that we've done over the past year, so whatever has been some of the more significant publications and we have sought to create a panel session that discusses that work. And we've actually explicitly reached out to other members of the community, not just SSAC members, we've always had a couple of SSAC members on the panel, but we've reached out to others out in the community to participate in the panel and to talk about the work in some form or other how it's been part of what they've done or what they're doing with it, or what they might do with it or what they might do with it in some case, it's a planning kind of thing.

Actually I was the one who organized it the past three years, but this year it's Paul Vixy from SSAC and Andre Rovachevski who will be from ISOC who are the principal organizers of the panel session that we're doing this year and they'll focused on DNS blocking this year will be the topic of interest.

Patrick Jones: Well, we've gone through our slides and we've had them scrolling for those that are remote and we've provided an overview of what our programs and activities and some of the things that we're focused on. I know there aren't that many in the room and there are some that are remote. If you have questions feel free to post them in the chat. There's another question in the room.

Marilyn Cade: My question is about budget. The Business Constituency chairs the budget working group for the Commercial Stakeholder Group and we're very concerned that the budget adequately supports certain functions that we think are very fundamental, compliance and enforcement, we're very articulate on. But we're also very interested in whether the budget that's just been passed regrettably since we had hoped that we would still have an opportunity to comment on it at the public forum, which is why I make that comment here, but we're very interested in whether the budget is able today really provides us with what we need in terms of scaling up to deal with the education and awareness and this is one of the key areas SSR for the folks who are I think possibly going to start arriving sort of in a flood by Toronto.

And I'm just wondering if you feel like you have the insights it's hard to forecast what the needs may be that are incoming, and yet the budget is already frozen. So looking ahead and beginning to plan for next year I'm just kind of interested in whether you have some ideas on how to forecast what those expanded needs may be.

Patrick Jones: We're actually trying to evolve a program that we've been growing over several years for law enforcement and in the past we've had a law enforcement day and it has been a closed session and that has raised some concern in the community about whether ICANN is getting too cozy with law enforcement and the like.

We started to think about ways to kind of separate that and this meeting in particular one of the things that we did was we actually ran a training day. And it was education that was focused on cybercrime and focused on the relationship between the DNS and ICANN and registration services and cybercrime and law enforcement and there's a very, very large body of that material that would be applicable to the broader community.

So quietly and gently John and I have been pulling some of the law enforcement people who are influential in that community aside and saying you know it really would be good if what we could do is figure out a way for the broader community to also participate in that education and in that environment, the law enforcement people can sort of put their Chinese wall and not talk among each other about investigations but they can come and talk with the community.

And in fact we had some really, really good dialogue on Sunday between some of the registrars and some of the law enforcement people on issues that you know a lot of people in the room just didn't understand and at the end of the day, there was much more crystalized understanding of resellers as an example.

So in Toronto and in fact at 9:00 I'm going to meet with the RCMPs the Toronto Royal Canadian Mounted Police are very excited about hosting something much bigger and one of the things that we're going to ask is if we could create some sort of pre-registration model where we guarantee that the law enforcement people for whom we're running this, can have a seat, but they'll also be some other you know first come first serve, no lottery, no archery, kind of activity where we'll get at least 50, 60 people more in the room who could come from any of the communities and then we'll go to all the SO and AC Chairs and say here is the registration period.

So hopefully that starts to address this, and I've been an educator for 20 years, John's an educator, we can do this very quickly. We have enough material to teach people for six months. So I'm sure that we could open up a college.

John Crain: Yes and when it comes specifically to what you're asking about budget, we have a very rigorous budget process on our team, and Patrick's our whipping boy to deal with the executives here along with Jeff. We try to ensure that we also build in a level of flexibility, so I am comfortable that we have enough budget to deliver as much capacity as we have, and we'll be flexible to change where we've focused – if we see

developments and needs. So if we do see an onrush of people that needs some form of outreach towards them or education around SSR, then we will make that happen. I don't think budget is going to be the issue, and we're going to need to close up, so Patrick if you want to…

Patrick Jones: We're kind of at the end. I just want to thank everybody for either participating online or coming here in person. We'll be around obviously until the ICANN is over, and leaving on Friday. So if you have any questions or you want to talk privately one on one just feel free to approach any of us, we're very open. And if we can't answer a question for any reason, we'll just be really honest and up front and tell you.

So please take the time to approach us if you have any other questions or send us an email via our security page and thank you for participating.

[Applause]

[End of Transcript]