PRAGUE – Commonwealth Cybercrime Initiative Workshop
Monday, June 25, 2012 – 15:00 to 17:30
ICANN - Prague, Czech Republic

Alice Munyua: That way we can have discussions, thank you. Well, thank you. Good afternoon, everybody and thank you very much for joining the workshop of the Commonwealth Cybercrime Initiation here at ICANN Prague. The current workshop will follow similar footsteps to the one we had at the Costa Rica meeting in March.

To begin with my name is Alice Munyua from the government of Kenya and I'm currently serving as the Chairperson of the Commonwealth Cybercrime Initiative Steering Group which is a multi-stakeholder pillar of this initiative.

It is a great pleasure to welcome you all to the CCI and thanks to ICANN for providing the space and support to have this workshop. I'll start by briefly telling you about the initiative or the objectives of the initiative.

The development of this initiative was driven by the exponential growth of the internet and of course the ardent need to enhance the global fight against cybercrime. Currently we have nearly two billion users connected to the internet and that is obviously is expected to rise by five billion in 2015. So the cost and lack of productivity for business and cost by increasing criminal activity online is something that needs to be addressed through global effort and collaboration and the Commonwealth has thought to play its part in this.

The Commonwealth is an institution of about 54 countries sharing the same language, on institutional setup, and it can leverage these commonalities to speed up and fast track assistant especially to developing countries and regions within its membership and beyond.

We have a model of computer and computer-related crime which can act as an official tool kit for countries requiring to implement legislation, and the model also enables countries to harmonize the global standards in relation to cyber criminality.

A proposal for a Commonwealth led initiative was first presented to heads of government at the meeting last year in Perth, Australia to help countries gain the necessary capacity to address cybercrime by way of policy, legislation, technical and institutional capacity. This was then endorsed at the meeting in Nairobi in 2011, and the initiative is currently moving from concept to implementation and I think we have a lot to report on that with the next speakers.

The government structures have been formulated in a constitution and a statement of purpose and the initiative is now moving forward with an in country project and request received through established networks of the Commonwealth.

The initiative has enjoyed a long consultation process last summer leading up to the IGF in Nairobi and through this process we have forged very many improved partnerships with approximately 20 members so far, which include the CTO, the Council of Europe, ITU, and of course ICANN and others. Our partnerships include governments, industry, not for profit organization, and it's this collaborative approach that the initiative aims to decrease duplication of efforts and

maximizing the resources that are available in a meaningful and sustainable way.

So I would like to now welcome – or before I finish, another issue is just the government structure of the initiative itself, it has three pillars which consist of steering group composed of various representatives from partner organization, an executive management group composed of representatives from contributing and noncontributing governments, the Commonwealth Secretariat and the Secretariat hosted and managed by COMNET Foundation for ICT development. As briefly mentioned earlier, the initiative already received several requests for assistance, and the initiative is currently working with the government of Ghana and we're going to hear a little bit about that. And we have other requests from the Caribbean and Pacific regions as well which are currently being evaluated and negotiated.

So why are we here today? The purpose of this meeting is mainly just like the other one; the similar one is to raise awareness of the initiative among the various stakeholders, amongst governments and law enforcement agencies so they become aware of the possibilities and functions of this initiative and how to exploit the assistance provided by the initiative itself. It's also an opportunity for new partnerships to be forged, and through the discussions, we can better shape the program itself as it continues to evolve.

The first half of this workshop will focus on presentations outlining the agenda, I'm sure – I don't know if you have the agenda with you, or it's going to be cast up there, and Tim will speak about the value added, then Joe from COMNET will provide us with any insight on the current

status of the initiative. Dave from ICANN will present a contribution on the Caribbean and Teki will provide a government perspective from the government of Ghana.

After the discussions we hope to address the topics of how members of the audience can contribute and become part of this CCI and how to encourage governments to take the initiative, the technical resources and capacity of the CCI, and finally areas for further development of the initiative. So and we'll be very happy to take questions as the discussions progress.

Finally, after the discussions, Lara from COMNET will go through the process of formally requesting assistance from the CCI. Thank you so I'd like to welcome the first speaker, Tim over to you. Thank you.

Tim Crosland: Thank you very much, Alice. Good afternoon, I'm Tim Crosland from the UK's Serious Organized Crime Agency, and we're one of the partners to the CCI, and this is really just a short presentation on why we think this is a valuable approach in terms of working together to develop a safe cyberspace.

A lot of people's first reaction to hearing about the CCI is not another new organization looking at cybercrime, and in some ways that reaction is complete correct, this is another new organization working on cybercrime, it's a new multi-stakeholder approach to developing a safe cyberspace internationally, and really what's it's about is drawing together the existing capacity of organizations that are already out there and providing a way for organizations like ICANN, UNODC, Council

of Europe, ITU, CTO and many others to collaborate in an effective format.

One of the new approach requires I think we all recognize why the task of developing a safe cyberspace is now seen as being absolutely vital not only to national and international security, but also to the realization of the millennium development goals. As ICT is seen as central to developing economic growth, we see a risk for certain countries that promote their critical national infrastructure using ICTs because if those can undermined quickly because the states don't have experience of dealing with cybercrime, and cyber security themselves, the Central Program for Economic Growth centering around ICTs may in certain circumstances even backfire, so that where cybercrime takes hold, it ends up damaging the reputation of the country as a whole for a place for investment and growth.

Clearly the task of working together to keep pace with the reliance on ICTs is an immense one and that is what makes it so important that the available resource that we have is deployed in a way that is efficient, intelligent and sustainable, and sometimes it's not always been clear that that is the case, there is a pressure on a lot of organizations to show that they are doing something to assist internationally and the question is often, well, where do we start?

We've got a budget, we've got a mandate to do something about cybercrime, we've got to show that we've done something at the end of this year. So that sends out some people to train law enforcement wherever it is, that set up a new laboratory. But without a framework and without a context, it's not always clear that these good intentions

do that much more than making people feel good, because if you're training law enforcement for example at a point when they don't have the relevant legislation in place, is that necessarily really going to be helpful? You're training them on laws that they don't have.

If we assist and put in a forensic laboratory at a point at which we really just don't have the expertise in the country to use that in the right way, it may not come to very much.

So how does the CCI aim to achieve this sort of coherent approach? Essentially it's a simple concept providing a platform that brings together all the major players in this field so that common priorities can be agreed, duplication can be avoided, and different mandates can be pursued in a way that is complementary.

Who stands to gain from CCI? This is a slight rhetorical question and the short answer is really everybody wanting to use cyberspace for lawful purposes, so that is both the requesting states for whom a safe cyberspace can mean security for their critical national infrastructure where they're dependent on ICTs, an environment in which key government services can be delivered online, an environment attracting investment and promoting innovation and growth. But also the wider international community benefits insofar as cybercrime, as we all know presents a common threat wherever it is based.

Who can make a request to CCI? Well, CCI is aimed principally at Commonwealth States which would benefit from assistance and international experience in developing their defenses against cybercrime, but CCI does aim to avoid hard lines wherever they get in the way of common sense. I think perhaps one example of that is the

division between cyber security and cybercrime, one can have lots and lots of interesting discussion about that, but when we get into country and we're looking at things that make a state vulnerable to cybercrime, well cyber security is clearly on part of that.

Good cyber security helps prevent cybercrime. So we don't want any hard lines around that, and in the same way where we get a request for assistance in developing a regional approach, perhaps where the region consists of a number of small states, CCI's constitution allows it to provide assistance across the whole region regardless of whether all the states happen to belong to the Commonwealth.

What can CCI help with? It will look at specific queries such as a request to assist with establishing a cert to conduct a training and resource needs analysis for law enforcement or a review of legislation, or it can deal with a sort of general query that says we feel – we need some help in getting things right around cybercrime and cyber security, not quite sure where to start and we'd really appreciate some assistance just in getting our strategy right at the outset.

But in either case, the one point that is absolutely critical is that all assistance is contextualized within a national strategy which indicates the value and sustainability of the assistance and commitments on the part of the requesting state.

Just imagining the conversation does start with a sort of we've got a problem but we're not quite sure what it is and how we go about solving it, CCI has developed a comprehensive checklist of all the different kinds of things that one needs to look at and this can provide a basis for the discussion within country stakeholders. So we might talk

about elements such as the role of the national cybercrime strategy, securing nationalized ICT infrastructure, implementing a national search, review of legislation, a training resource needs analysis for law enforcement, et cetera, et cetera.

So how does this all work in practice? If a general request comes in CCI might consider sending out a scoping team to conduct a gap analysis and that will be really assessed against the checklist. Depending on the circumstances, the team might consist of experts covering a variety of different bases; you might have a security expert, somebody with an in depth ICT background, a law enforcement officer, a lawyer, whatever we think we need.

And then the scoping team will prepare a report analyzing where further work is required, and this is really designed to help states in requesting more specific forms of assistance. And that then puts CCI into a position that it can coordinate across its partners. So we say look there's a request here to forge links with a university to help develop the research capabilities and training capability in a country, is there a partner who can help with that side of things? There's a request to launch a public awareness campaign around cyber security, cyber hygiene, have some got experience of that? Someone we can put the state in touch with.

How will work be funded? In the first place as far as possible the idea is to coordinate existing mandates and funding streams so the first question is well how much of this can be done in kind, because we've got organizations out there whose job is to provide this sort of help. In some cases, clearly there will be a requirement for funding, if the state

itself hasn't got the funding available, then CCI can assist in securing funding from relevant bodies helping to draft tenders and this sort of thing.

This is a question that's been asked a few times, why the Commonwealth? And it can seem like a glass half empty type question because well you know this is something, this is really quite a lot of the planet in a way, 55 states I think at the moment. But the short answer, the sort of factual answer to that question is that this is a project with origins in the Commonwealth, with origins in the Commonwealth internet governance forums as Alice mentioned earlier on, and in fact it was the Commonwealth heads of government in Perth last year, who expressed that commitment to improving international security by improving legislation and capacity and tackling cybercrime and other cyber space security threats including through the Commonwealth Cybercrime Initiative.

There are some advantages in starting off working in the Commonwealth, we've got the common legal traditions, the common law, also got the model law and the [Harreri] scheme, common language, but I think this is really important, and this is just a starting point. It is the first time anyone has really attempted to do something on this scale in this field. And if it continues to work as it's currently doing well clearly it is a model for a more global approach. Okay, thank you very much.

Alice Munyua: Thank you Tim. And I would like to call upon Joe Tabone next.

Joe Tabone: Thank you very much, Alice well much of what I was planning to say has been covered already, so I can probably go and have my nap this afternoon. But I'll add a little possibly maybe helpful if I really added a bit of context to the initiative of how it came about and then the purpose of my session was really to give you the status of where it's at.

So just starting a little on going back on how this really started probably four years ago, the Commonwealth Secretariat as really part of an ICT for development program thought that given the increasing prevalence of the Commonwealth of the internet in our lives it would be a good idea to set up a Commonwealth internet governance for the purpose for setting up such a forum was again with an understanding that unfortunately a number of Commonwealth member countries are not able to or adequately represented at internet-related forum whether it's ICANN meetings or at the IDF.

So the purpose of the Commonwealth IDF was it had the objective of anyway trying to draw really member countries into some of these focuses where they were not able to that the Commonwealth IDF would provide outreach to these countries by really informing them of developments and in the course of the setting up the Commonwealth forum, we also made an attempt to engage stakeholders in order to get a sense you know from them about what they saw as the really major public policy issues that were concerning them. And this we did at every opportunity that we had the Commonwealth itself organizes a range of training and development activities on different continents.

But we also have been having these workshops in order to set up about four years, and really consistently when we have these discussions with

stakeholders about what they saw is a major very public policy issues, you had sort of the same litany of issues effectively being articulated, and these had to do with access, it was a really major issue that invariably came up. Another one had to do with content but two major issues that were always at the top of the concerns of the people were the security of the internet and one aspect of that is also really child protection.

And in the very course of our deliberations I suppose, the Commonwealth worked on really how to deal with this concern. We knew that there were a lot of conferences, talk shops relating to the subject. I think of the past two or three years, there has been an attempt again on the part of the Commonwealth to introduce modules having to do with internet governance and the issue security.

But in the end the Commonwealth saw the need for something that is really more coherent I think along the lines that have been described by Tim. I think on the one hand there really was there really was an understanding about the multitude of activities that were taking place you know all over the globe by way of training that was being provided really most particularly to law enforcement agencies and to prosecutors and to judges.

But much of really what was taking place was and this is really not an analogy but it's really the observation of the people that we're talking to that the activities that were taking place, were you know fragmented, they weren't really part of some really broad picture that was of a country that was looking at the needs, really starting with the legal frameworks that they need to have.

So the concept of really a comprehensive and coherent initiation came as a result of this feedback that we had with stakeholders and as a result of that there were a number of really countries that a task group was put together – a work team was really put together with many people who were involved in the formation of this concept sitting around this table, a representative from the UK, from Canada, representatives from Sri Lanka, we had Zahid who was one of the prime contributors really to the initiative.

So that's really how the concept came about, and the other factor I suppose that contributed to the Commonwealth trying to come up with something that is more coherent, comprehensive was the sense of duty that there is that the internet was just changing so rapidly, and particularly the growth that we're experiences and that we envisage in a short while as a result of the internationalized TLDs and now the expansion of the genetic space where we've seen as was being said this morning of really an internet with about two billion people accessing it really today, that this will probably double. That's taken about 15 years to achieve that, it's going to take 12 to really 24 months to double that.

So if security was an issue yesterday, this assumes a far greater urgency today, and so that is the context for this, and the driving force behind this initiative. The other point that I wanted to say about this is that the Commonwealth in taking this initiative was doing this and sort of making an issue in that the Commonwealth is an organization by the Commonwealth here, not the Commonwealth of member states, but the Commonwealth Secretariat has little by way of inherent capacity really technical to deal with this, but what it was sought to do in this is

to join entities, organizations that historically have had the capacity in this area or the resources to contribute really to it.

And so in the course of this and really as part of the formulation, the Commonwealth are doing really a number of very critical partners who have been prominent in some contribution to the cybercrime and cyber security capacity building. These were the Council of Europe by virtue of the early very global convention that was on cybercrime today, the ITU by virtue of the historical mandate having to do with telecommunications and the tool kit that they have developed for regulators, but also a tool kit really on cybercrime, but additional capacity that ITU has by way of providing really substantive technical support to countries in a range of capacity building activities.

The initiative is about the internet, so a principal player in that is ICANN. So ICANN is really one of the partners in the initiative which has much to contribute and is actually contributing much to the initiative as we speak, and I think David will be talking to us about this.

So in all the and this is again really part of the uniqueness of this, there are really 25 – about 25 different organizations that are involved in this partnership, each really contributing something to it, by way of expertise or other type of resources. So that is the background to it, and now we're in the process of translating this into really some substantive reality on the ground.

I think that the challenge that there is in this is significant. I think it's really probably a threat that we have probably chosen not to speak about too much in the past. And I was a national regulator for really about eight years and on the one hand, I was very much driven by

promoting connectivity to the extent that that's possible for the citizens and for the general public. At the same time you know I also understood, recognized some of the inherent really downsized security in this, but I think that we're now at a stage where there is the need for some very, very significant capacity building in a number of countries.

Where we are in the translation in this is – there is as Alice mentioned a government structure that has been developed now which really consists of three parts. There is a Board which we call an Executive Management Group and that is drawn from governments who are contributing in a financial way to the initiative and in addition to that there is the Commonwealth Secretariat who is a member of that Board. Then the really substance of the initiative is a steering group, which is chaired by Alice and the steering group is drawn from all the participating agencies, so there are about 25 here sitting around this table. This is the group that identifies prospects and they group who will be contributing capabilities to the initiative.

And then there is a Secretariat which is the Secretariat of services invited by COMNET which is an international foundation which is set up in Malta. With regards to the specific project activities prospects there is the first project that we've been working with and we were very interested in using as a pilot is in Ghana, and I think that we have a representative from the government of Ghana Teki who will be speaking to us about that. The government had invited us first to assist them in the development of a national strategy on cybercrime and as a subset of that the government was seeking assistance with the setting up of a national cert. So I think that will provide some details of that.

Then projects and prospects, the last several but two major ones that we hope will come on stream in the next short while, as a matter of fact they have been the subject of some very, very considerable discussion in the last six months. One is assistance to the Secretariat to the Pacific in the drawing up of a regional strategy for cybercrime and a similar initiative this time working with the (inaudible) telecommunications union for similar assistance in the development of regional strategies, I think are the two instances.

The regions by virtue of the geographic makeup, the number of sovereign countries, the size of some of these countries, the distance and lack of really capabilities they have, there's a recognition that the eminent logic in addressing some of the capacity requirements on a regional basis that it may not be very cost effective to try and develop some capabilities given the size of these countries at a national level. So that's the logic – the arguments behind the regional report, and the regional approach is really a choice of the region not one that is in any way being imposed by the Commonwealth.

And then there's another very specific project in another African country, it wouldn't be appropriate for me to mention it at this particular point in time. I think with respect to the Caribbean region again, there's as recently as two weeks ago, there have been two meetings, two Minister's meetings one in December and one about three weeks ago on the subject, broad subject of ICT for development, but then very specifically a good part of the agenda was given to the aspect of securing cyber boarders and there's a consensus in the Caribbean about the regional [purge] or the consensus on the criticality of collaboration between the very different countries, and also

capitalizing on the goodwill of the many multilateral agencies who are interested in provide their assistance.

Having said that it's also recognized that it may be difficult to get all the countries signed up to working on all the regional strategy and I think that the approach that is really being adopted is that there have been a number of countries probably about six of them who are ready to start working on the strategy and there's a follow up meeting that is being convened now for this coming August, where hopefully there will be a framework with specific objectives that will be developed and timeframes.

So I think that's about where we are with this. I had a note here about how to encourage take up, I think that Tim spoke a little about that, one of the reasons why we have this type of sessions is to develop as much awareness about this as possible and we use a range of vehicles for that. So anybody here is interested in any additional information, we will be very happy to provide that. And Lara will speak later about you know how requests are made. I think one of the things that we make as a condition in this is we want to make sure that there is a political commitment before we deploy any resources to this and then that the recipient country is also committed to freedom of expression and human rights.

So I think I'll pass this onto now to Alice, yes, and I'll be happy to answer questions later. Thank you.

Alice Munyua: Thank you Joe. I'd welcome ICANN's Dave to give us a presentation on ICANN's contribution so far. Thank you.

Dave Piscitello: My name is Dave Piscitello. I'm the senior security technologist at ICANN. And I would like to share with you today the ICANN perspective about the initiative, and provide a status report of some of the things that we have attempted to bring to the initiative since our participation began I began I believe last December.

One of the important and initial observations I made when I first participated with the steering group is that there is a great deal of synergy between some of the things that ICANN considers its core values with respect to our own governance area which is internet name system. We believe that the initiative will enhance operational stability reliability and then security of the internet. And this is one of our core values, and it's a very important one for us, in fact we have an entire program called Security, Stability and Resiliency within the ICANN community that is driven largely by my security team which is led by Jeff Moss. And so we looked at what the CCI wanted to do and we saw that there was a fairly great deal of overlap, and the complement that we saw in the kinds of education and training in particular for DNS operators was a very nice fit if not a dove tail.

Having come from private sector, one of the things that I observed over the many years that we had to fight this battle with relatively little participation and involvement from any governments, is that one of the keys to success, one of the most important keys to success is agility. I mentioned this probably so many times during a CCI meeting that

people are tired of hearing it from me, but the criminals are must faster than we are. Picture Sir Francis Drake and his tiny little privateers fighting the Spanish Armada. Well, we're not the privateers, we're in the large ships that are not moving very fast, and we're getting killed.

So one of the things that I've been emphasizing that is we need to spend less time in discussing how to do things, and more time in actually executing, and so I've been most of my career get things done and ask forgiveness as opposed to permission. I'm not sure that that actually fits very well in governments, but it actually is important so for somebody in the room to say let's get this done.

So one of the things I hope we can do and I think we're starting to exhibit is try to help a relatively large process move at least with some agility in areas where we already know as Tim pointed out that there is an opportunity for in kind of participation.

The second thing that I think is very; very important is I think within the Commonwealth there is a baseline of trust that is absolutely essential in order to solve any problem especially with cybercrime. The private sector especially with work with law enforcement over the past several years, there is a tremendous amount of personal contact and trust that's necessary to grow these things. And so I was very happy to see that this is an important criteria for the CCI, and I think that one of the things that we might be able to do is lead by example, and I think if the Commonwealth countries can go and they can cooperate and cooperate as well with companies or organizations like ICANN and others then other nations may follow and I think that that's a very important objective for us.

ICANN is a non-government agency and I in particular am not a citizen of a Commonwealth nation, but one of the things that I think we also want to do is demonstrate that this is a global problem and it's going to be solved reaching out beyond borders and grabbing people with expertise and with willingness and energy to actually try to solve the problem.

So in that spirit and one of the things that we promoted when we came back to ICANN and talked about what could we do was we already do capacity building, this is part of our mission, it's part of our budget. We provide DNS training programs for ccTLD operators, we provide DNSSEC training programs for operators and we are engaged very, very meaningfully with the broader security community with organizations like the Anti-Phishing Working Group, the Messaging Anti Abuse Working Group, it should MAAWG by the way and others. And we work with many law enforcement agents, we visit law enforcement agencies whenever we have the opportunity we share our training material and so I think that we have a fit here because this is right in our wheelhouse, this is one of the things that we do and we try to do well.

I also think that it's going to very important for the Commonwealth and for governments in general to understand the importance of working with the private sector and not only because the private sector has a role, but because the private sector has an incentive. And I would encourage the Commonwealth to in particular think of not about all the private sector partners exclusively as a source of funding and equipment and training, but also to understand that they have an incentive that is not always obvious.

I mean one of the things that is most challenging for multi-national companies for global presence companies is that they're victim to the lowest hanging fruit. So the weakest of the countries cyber security is going to affect them and that's where you're going to find the locust of badness so to speak, or loci of badness, because there's more than one.

So one of the things that I'm hoping is that we can start to think globally from both a public and private perspective of increasing what I call the global security baseline. Every time we raise the level of security of I don't want to say worst offenders, but it's applicable, of the worst offenders and we eliminate some locus of badness on the internet, we help every single company, every single nation, every single citizen. So I think that that's a very, very important factor in what we're trying to do.

So what specifically is ICANN going to contribute? And Tim's phrase is in kind participation, I call it sweat equity because I came from sort of the startup environment where you come in, you work 1,000 hours a weeks, you know your wife and family leave you or can't remember you when you walk in three months later, but you've taken something from concept to inception.

So one of the things that we do have quite a bit of very senior talent and leadership in is the DNS and internet security expertise; my group alone represents and I think there's six of us and we represent nearly 125 years of expertise. And so not only do we have that to lend to the community, but we also have a different perspective, because many of us have already had to tackle this from a private sector perspective.

And we already as I said offer DNS training as part of our capacity building for the broader internet, and what we intend to do is try to

focus a significant amount of that on helping Commonwealth members at least in the near future, at least in the near budget, this is where we intend to direct a significant amount of our effort.

We do two kinds of training in particular. We go to an operator and we help them build out their infrastructure, we teach them essentially how to run a name server, how to manage the name server, how to secure their operational facility from physical level to hardware through to the virtual or what people call traditional internet security, we then also encourage DNSSEC deployment because one of the things that we're very keen to do is to try to improve trust and confidence and accuracy or integrity in the name service because it's such a critical component of every single transaction on the internet. If you can't resolve a name to an address, you're basically not going to work very well in today's internet with millions and millions and millions of websites and mailers and the like.

So we have this shared objective, and one of the things that we hope is that by our participation we actually help our own community because it will grow. We think that we will be able to see a value in bringing existing registries that are not as robust and secure as some of the larger registries that have been in place for decades, the COMNET and org registries as an example, and also info and biz and the like. We feel that when we get this baseline up we'll have a much more resilient and effective global DNS.

We also think that as we manage to sort of complete our cycle and the last delivery of what we would do in training is to help Commonwealth members assign zones, we build out this trust model throughout the

entire Commonwealth, so one of the personal objectives I would place for ICANN and what I would think would be a tremendous win is that we have every Commonwealth country with assigned TLD zone within a reasonable number of years.

The other thing that we try to do that is I think critically important to understanding how this all succeeds is when we work with an operator, we try to introduce them into the global network of operators, we try to bring them into the club so to speak. We want them to build out their own confidence in their system so that they can go and they can participate as peers with the rest of the community, can go in a room with the folks at VeriSign with the folks at [Ophelius] and they know that their practices are good, and they know that their product is good and that respect and that recognition and trust actually works really well, because then when they have a problem or an issue, they know exactly who to go to, they know exactly what kinds of responses they can get. And they can also continue to sort of pay it forward. They can use it to help build capacity in other Commonwealth nations.

So I think that there's a lot of sharing that can go on here. So let me tell you what we have done thus far. From June 11th to the 15th the CTU actually held an event called [Carabnog] in Port au Prince, Trinidad. And cooperating with COMNET and the CTU, ICANN brought some of its training people and programs to the conference, we designate an entire day for DNS training, and we did four modules of what is normally a very, very large set of training programs.

We taught some DNS basics, we provided the fundamentals of DNSSEC and we provided an in depth DNSSEC session, and then we did a signing

demonstration. Now a signing demonstration sounds like one of these canned demos at a conference or a trade show. Well this is really much more than that, because one of the things that we try to emphasize is the criticality of actually having a very, very secure and trusted signing, because the cryptography that is used here is essential and compromise are the keys in the cryptography is a catastrophic event for TLD operators.

So we impress on them that there is going to be some physical provisioning there is going to be some extremely important functions associated with the signing that are critical. And so we start to put them in this mode of cryptography is very cool, cryptography is very important and we turn them all into geese, so that's my goal is to have everybody become a nerd by the time that we're done.

So we had 50 plus people in attendance. We also had some remote participation. I'm very encouraged that the remote participation was present and I think that we're going to try to encourage that in the future for whatever we do. We will attempt to follow up with this training with more successor training this is not what is euphemistically called a one and done, or do it once and forget. In security, in networking in an operational level, repetition is the key to learning.

And the more that you do these things the more that you're exposed to the technical side of this, the stronger your operations can be, because then things become rote. You know instinctively when things are going wrong. And it's like brewing beer, you know when to turn the temperature up, you know when to turn the temperature down because you've done it so often.

So we will continue to coordinate with the CTU, and with COMNET to arrange some targeted and longer and more formal training, so that we build capacity in the Caribbean region, you know it's a challenging region because of the geographical diversity, it's a challenging region because of some of the VISA problems we would have if we try to bring many of these participants to the United States or to Puerto Rico or to someplace else that would be more convenient for us.

But we'll get down there and we'll figure out how to actually overcome that and we have people, I believe Richard, Richard Lam is here and so is John Crane. Both Richard and John performed the training, they're very familiar with the on the ground people at [Packer] Clearing House who are very instrumental in how the CTU operates, and we're going to have some really significant dialogue with them, when we finally settle down after this meeting and break in our new CEO.

So I think that what we can do, we can do quite a bit more in the region to improve what we've already done. And as I said one of the things that we'd like to start to do is train trainers or to prerecord and deliver the training remotely so that we can maybe make this a much more easily attractable deliverable to other parts of the globe.

So just to finish this is like proof positive that we actually were training, there's John in his not suit, this is John in his suit over here and Richard – by the way having John this is a singular event, I've never seen John in a suit and I've worked with him eight years. Richard has done a lot of work in the Caribbean and many of you if you go and you talk with any of the operational people in your countries and you mention either John

or Richard, you'll get very, very high praise for both of them, so we're really very happy to be able to bring this kind of talent to bear.

And I think that we've got a very good start. Our goal here is to give some early successes to the CCI and to allow them to go to countries and say look what we're doing without any money? Imagine if we had some. So with that if you have any questions, as Joe pointed out, we can answer them when we've finished all the rest of the presentations. Thank you.

Alice Munyua: Thank you Dave. I think I would like to invite the prospective from national governments. I'd like to invite Teki from Ghana.

Teki Akuetteh: Thank you Alice. From Ghana perspective we found the CCI initiative as an approach to deal with our cybercrime policy, because when we realized that the approach, the best way to deal with cybercrime which was baffling our country was to look at a multi-stakeholder approach that is to harmonize existing systems and legislations to ensure that there can be enforcement.

And we found the cybercrime initiative as a very good platform; because one, it brought together all the key partners that already government was engaged with. An example was the ITU and several other organizations that we were already working with. And to take it from there we wrote to CCI and requested that they come in. We went in with a specific request that is to help us with our set capability and what came back which is a good result was to have a scoping mission

with their team come into the country, look at what exactly is happening in our country now, and as a result of that, that's scoping mission we had some key revelations which was very good for the country and government in terms of a holistic approach to dealing with cybercrime within the country.

One of the main areas which I'd like to share with you that came out it was our need to finalize and put together our policy and strategy and for this we are going to look at the next steps which involves CCI with a team that already government has engaged on the ground to see how best we can collaborate. The important thing is that CCI bring some more experts which either to we do not necessarily have who can come and share their own experiences with us. So to a large extent we do not have to reinvent the wheel in implementing our cyber security strategy and policies. But our people on board with their team can come up with an effective system and policy that can be best implemented in line with global best practice which is the government of Ghana's policy in dealing with cybercrime.

We also going to go ahead with the set capability assistance which is something that we had started working on with the ITU. And like I mentioned in both the multi-stakeholder approach that CCI brings, it was very helpful because the ITU was right there with us to pick up with us from where we had left off. And brought back at least the process that we had started which we had able to not finished, and so there was no duplication of efforts by bring CCI on board, because all these partners were there to help us implement from wherever we had left off with the ITU.

Also another thing that we looked at was the legislative front. It was quite revealing through the scope mission our country has tried over the last four or five years to put in key legislations to strengthen cybercrime implementation. And what we realized during the scoping mission was that a lot of the agencies that are either supposed to be enforcing or implementing the laws, did not find the laws to be adequate. And these were all questions that came up. So to a large extent within the countries, the government thought that there would be the need to actually review the state of those laws, to see if they're really adequate for our purposes, is it just an issue of those implementing who do not really understand, and these are some of the benefits that we have gotten from these processes.

Also enforcement issues was very big, because we gave CCI the opportunity to meet with key agencies of government that were doing enforcement of cybercrime issues. And it was quite obvious that we were not getting the best; one because they lacked the necessary training and all of that, and so this was one of the key areas that government thought it would be very good if we can collaborate further with CCI on this initiative. The reason being that with all the partners on board, we can bring to bear experts in this area who can actually assist the country where we fall short in implementing some of these things.

To just end it all, I would just like to say that for the government of Ghana, the benefits of aligning with CCI in the implementation of our cybercrime initiatives was at least the benefit from similar legal systems and institutions as a result of our Commonwealth, the similarity of the language, the ability to collaborate with the several partners, some of which we've already been engaged in, so as not to lead to duplication of

efforts in that area. And to a large extent, CCI to us is more of a one stop shop to dealing with our cybercrime issues. I think that would be it, thank you.

Alice Munyua: Thank you very much. I would now like to open up for discussion with questions and comments from the floor. Uganda.

Ambrose Ruyooka: Thank you very much here. Everyone to once again appreciate the initiative of CCI. I said this in Costa Rica that this was happening at the right time, when most of our governments are [asking] how they went through a process that has actually been described by my Ghana colleague.

In Uganda, a year ago we enacted a set of [follows]. It appears transaction was low and the flexibility is low, the competency is low, and production of communications and all these were geared towards (inaudible) as one of the objects. But one year down the road, the alternatives. We (inaudible) have actually been foretold, because when this was being passed, it took ten years doing the process because there was lack of capacity in the people that are involved in the process of [formatting] the laws right on up to our Parliament.

And now we're having challenges with the other problems: investigation, the litigation, the constitution, the judiciary, they all seem not have taken up the issues that are aligned therein. So where I'm coming from now is I heard about this three months ago, and I'm hearing about it again now when I'm at ICANN meeting, back home over

the last three months, who I talked to about the CCI that would maybe have known about it, know [a way] about it? So I'm wondering the mechanism we will place to communicate with the national stakeholders. The national stakeholders of course they are open to different models and there is no way in which this can happen without establishing national contacts within the Commonwealth countries.

I don't know if it is through the Minister of Foreign Affairs because some in some of our countries the ministers represent asset to Commonwealth Secretariat; or if we could do it through the Ministers in charge of the [community] or something like that. So the mechanism is what I want to see how this can be communicated proliferate down to the stakeholders because the key issue is awareness and I am glad that you're saying that this will be a presentation of how people can access information for customer support and things like that. So I'm looking towards the mechanism that we'll create in accordance with the Secretariat and the participating countries, certainly (inaudible) have already written down. Thank you.

Alice Munyua: Thank you, very good question. I think that's an issue that the steering committee and the Executive Management Group will have to think about. But I think off the cuff outreach and awareness is going to be a key area of the steering committee and the Secretariat will have to put in as an added activity in terms of just reaching out to Commonwealth countries and others as well in terms of creating awareness regarding the initiative and the tool kit itself. Yes, Mark.

Mark: Carvell

Thanks very much. That's a very good question and obviously one that concerns us all on the Executive Management Group. I'm on the Executive Management Group for the UK government, we're one of the funding facilitator governments for this initiative, and we certainly want to make sure that there's efficient means available to us to communicate what the initiative provides in terms of opportunities for stakeholders, for governments, for law enforcement, for judiciary and so on and every Commonwealth member state. I mean there are some obvious ones, there are the internet governance [fora], the regional [fora] which involve Commonwealth countries establishing some linkage. If resources allow to be present, to have visibility, to speak about the initiative at those fora and that national fora if we can look at what's coming up over the next few months and so on.

But it would be really valuable to help us in this formulation of a communication strategy to hear from people like yourselves, I mean do you have a particular suggestion with regard to Uganda and other states, how we can ensure that communication is valuable? So if you've got some suggestions for us, please do follow up, and we'd really appreciate that from the Executive Management Group. Thank you.

Alice Munyua:

Yes.

Zahid Jamil:

Thank you, [Zahid]. I just sort of have a few comments about many of the presentations made and a question actually at the end. I think it's amazing how the way Ghana has sort of tiered out the various things, I

mean – off the top of my head, there's policy strategy, there's the cert, there's the legislation, there's the enforcement that took place and it's wonderful to hear that it was because of the similar languages that it helped. That really sort of ticks off so many issues that we sort of dealt with when the group got assistance. And even with the existing cert, with having had engagement from international organization, the CCI helps in re-energizing and re-establishing certain other efforts that exist. I think that's fantastic.

I was wondering if it would be possible to get Ghana to sort put maybe you to write up a one-pager or a two-pager that could be made available you know maybe on the ICANN website or the CIGF website. It kind of gives all the reasons you laid out would be a fantastic, an example that other countries who would come to future ICANN meetings about the Commonwealth or the IGF to know what were the experiences that Ghana gained from this.

And also the question raised by friend from Uganda, I think it's absolutely apt, the need for communication. My thought would be since we're dealing with cybercrime, that maybe a good inroad, a powerful inroad identifying that in Commonwealth countries the justice ministry tends to be a very sort of hands on, really does have a lot of clout whether it be the misuse of [interior] or with the law enforcement, et cetera and legislative drafting. That may be the first port of call really as a thought.

And moving to Dave, Dave excellent presentation. It looks like we're moving towards what we were thinking about, going a secure Commonwealth ccTLDs, this is a great project. I hope you know all the

success and best wishes with that. I was wondering what's the next event if there is to be any, what is the next sort of steps that you would be taking with more Commonwealth ccTLDs for instance to sort of have this. This is a great example that you just gave of an event that took place in the Caribbean. So how do we move broader to sort of more Commonwealth countries and if you had thoughts and ideas about that, I'd love to hear more about that. (Inaudible) continent for instance as an example. Thanks.

Alice Munyua: Joe and Dave can answer, yes, David please.

Dave Piscitello: So honestly, we're catching our breath. The whirlwind of dealing with new TLDs of a new CEO of trying to execute on what we promised before our budget ran out on June 30th, you know for those of you that don't understand. ICANN's fiscal year begins and ends on June 30th, and so we had a certain amount of money that we either spent or it disappeared. I've never understood that part of accounting, but so we wanted to spend it, and we were more than happy to try to apply it to the CTU and we managed to through Richard's coordination with some folks at Packer Clearing House and CTU, we managed to actually pull the rabbit out of the hat.

We still need to do a post-mortem and then to figure out what would be the next best kind of training to deliver, because we can bring equipment down, we can actually build things for people and give them hands on, and there's a lot of different kinds of training that we can do.

So I think for the near term, -- yes, I'll let John say something, but for the near term our focus is to try to continue to train in the Caribbean and raise that level and maybe made them a model for how we might proceed. So John Crane is going to just amplify.

John Crane: Yes, so I lead most of the training programs. We also work with many other partners and one of the things that I'd like to see is that when we're holding trainings with other partners that we work for the CCI to bring Commonwealth countries into those trainings as well. So I know for example we'll be talking to LAC TLD later this week about doing some training in the Caribbean where there are of course Caribbean – so we're going to look for as many opportunities as we can to bring Commonwealth countries into existing training and to apply any dedicated trainings that we can.

Joe Tabone: Yes, just to add a little to what has already been said in response to the gentleman from Uganda, we're here really for the next couple of days, and I think that we would like really talk to you specifically about how we are going to go about communicating with the right resources in your country.

I mean the whole purpose of this workshop is precisely to really get people to know about this, this initiative and then to follow up from there. Interestingly enough Teki is here today as a result of a program that she was attending a year ago in a (inaudible). It was something that's quite different but we had a session on VeriSign security, so that's

how the contact came about. We just finished really two weeks ago. We had a Commonwealth program, it was on regulatory frameworks but we have to introduce a module on this on internet governance and very specifically on cyber security, Zahid as a matter of fact was very much involved in the design and the actual facilitation of the program.

And apart from 30 participants from different parts of the Commonwealth, we also had some people from the new government in Libya. So this is how we are really making people aware of this, and if we can chat just a little after this, and then take it from there. Thank you.

Alice Munyua: Thank you Joe. Any other comments or questions? Okay, then I'd like to invite Lara just to explain how to get involved in the initiative. Please Lara.

Lara Pace: Thank you Alice. So the title of the presentation is how do you start the process to make a formal request, and Teki made reference to the scoping mission. So we see on the request the scoping mission, and that's level zero, but I think – level one, and I think it's level zero and you can start by contacting myself, you can do that through the COMNET foundation website, or the Commonwealth Internet Governance forum website. If you go to all the contact forms, they point to my email address. So I receive any communication off that website. And through a series of conversations we facilitate this formal request that Teki was referencing. A number of calls will take place

between us and yourself and partners that will be contributing to the work.

And the letter really is quite important to evidence the political commitment of this work that we will be talking about. That will take place through the CCI. And that's really the process, we start from there, we use different templates according to whether it's regional, it's country, whether the request is specific, it just emanates from a number of conversations that will take place.

So feel free to email me any questions. If you do come across a project description document, you will find my email address on the front of the document and also on the back, on the website anywhere. So I look forward to hearing from you.

Alice Munyua: Thank you Lara. Zahid did you want to add something?

Zahid Jamil: I am just saying what is the email address.

Lara Pace: Oh, yes, sorry, well my email address is [Lara.Pace@COMNET.org.nt]. But if you go to our website and the CIGF website, go to the contact form, you will be contacting me, you won't be contacting anybody else.

Alice Munyua: Yes, please.

Beran Gillen: Hi, my name Beran; I'm from The Gambia. I just had a suggestion and I don't know if it's a question or not but with regard to disseminating information about the CCI, I would suggest – I noticed you had a session in the Caribbean, with the Caribbean network operating group. We have something like that in African region as well, [AF] which is becoming very popular. It was recently held in the Gambia, we had people from 23 different countries in Africa. So that could be a way of also possibly you know disseminating information about the CCI. It could be a one stop shop in addition to the national face to face IGF as well as the regional one which is actually happening in Sierra Leone in a few days, so that would be a good start.

Alice Munyua: Thank you. Markus.

Markus Kummer: Thanks very much, that's very helpful information and I hope we can rush out a contact for this Sierra Leone national IGF, get a link somehow, a flyer or something, if we haven't already got that. But anyway, there is going to be a workshop on the initiative in Baku at the Global IGF just to add that.

And just coming back to the communication to Lara at COMNET, I mean I'm right in thinking Lara aren't I that this could be from any stakeholder community, it doesn't have to go through the government? I mean we're really open to proposals from anybody or any entity or community involved in the cybercrime area or contributing to initiatives

in the cybercrime or potentially wanting to and looking to the CCI to help with that process. I think that's – thank you.

Beran Killen: Yes, you're right.

Markus Kummer: And the other point, I guess at some point after that communication exchange some physical meeting would need to be set up, but most of the keys or the establishing the grounds for a potential project is done online, so there's no cost.

Lara Pace: No, we try to avoid as much as possible the cost. And yes, most of the conversations would be – I don't think a physical meeting would take place before a scoping mission. Like for example in Ghana, all the negotiations took place over the phone and online, and the letters were exchanged by email and also another thing I wanted to say. The Commonwealth has national points of contact throughout the whole Commonwealth and their national points of contact on the ICT 4D program that the Commonwealth runs. Now there are 48 national points of contact in the 54 countries, and I've just looked up Uganda's and Uganda unfortunately doesn't have a point of contact. It's one of the missing six.

But we keep these national points of contact up to date with developments and we try and drive information both at these

international conferences, international meetings as well as through the Commonwealth points of contact. Thank you.

Alice Munyua: Thank you Lara. Yes, please.

George Nyabuga: My name is George Nyabuga from AfriNIC, originally from Kenya, but now working in Mauritius. I just wanted to say in addition to what she just said that we host the [WHOIS, .ss] and we also have RPKI which is the (inaudible) instrument that can be used to enhance cyber security as close as we try to appreciate the efforts in fighting cybercrime. That we at AfriNIC are interested in such issues and we working very closely with various organizations including [AFNog] and including CTO for example and the Commonwealth in trying to enhance cyber security in Africa. Thank you.

Alice Munyua: Any other comments or questions? Okay, then I move to close the – oh yes, please.

Female: I just wanted to know whether in addition to obviously the support that you're giving in kind whether there are any financial support for countries who are interested? I may have missed that during the presentations.

Joe Tabone: The approach that we adopted in this is we first try to find out here what the needs are in those countries. We do advocate to the extent that it is possible, if the country is not very clear on what its specific requirements are, so the country may be aware that it needs the legislation or it has legislation, but it needs some training of law enforcement people or it needs some technical support.

So very typically what is done, what we advocate in this is for a very short scoping mission once we have an understanding of what the needs may be to try to get a sense of – a better sense of what is needed and the resources which would be required in that. And then one would go from there to deploying really a person or team of people to work on a strategy in conjunction with a country and it's that strategy – the purpose of the strategy is to tell you first of all what the gaps are with respect to security. Are the gaps not having the adequate legislation in place? Are the gaps really technical? Is it training of your police or national security forces or whatever that may be?

And in each instance there will be an attempt to get a measure specifically what would be required to address the legislative gaps that you may have, or the training to cost that, and then work in conjunction with you the resourcing of that will come from these partner agencies by way of technical support. And if there is financing of some these issues should be required, then we will work in conjunction with you to approach donor agencies for that. Does that answer your question? Thank you.

Alice Munyua: Zahid, please.

Zahid Jamil: I don't wish to say that the CCI because I can't speak necessarily on their behalf on this point of saying that there could be financing available, I think it really brings people together and I don't know whether any partners would like to fund things as they go on, but let me share certain examples in my region for instance.

When you have these sort of assistance that can provide you with scopings, you see a lot of times you go into a country, the country doesn't even know what it should need. It happens. It happens in my country for instance, unless that awareness is created. So once you have an output as to all right these are the things that are gaps, and these are the things that you need, the great thing about that, and that can initiate a conversation between your governments and say the World Bank for instance and others. And so a whole bunch of people can either be connected through the CCI or even otherwise, having obtained that sort of let's call it a raising of profile of certain aspects, those issues can then be taken up by the ADB if you're in the Asian region or other organizations.

So it does have that sort of impact, where otherwise these aspects or the requirements of fundings just never, never raise in profile and nobody even knows that this needs to be done. So I think that's what – and at least that much is a help to those things.

Alice Munyua: Thank you; I see no other requests for the microphone. Okay, I want to thank you all very much, starting with the panelists for the great

presentations and to all of you who have participated and we look forward to seeing you again during the next ICANN meeting and at the Global IGF. Thank you.

[End of Transcript]