CR - Fellowship Morning Meeting
Wednesday, March 14, 2012 – 07:00 to 09:00
ICANN - San Jose, Costa Rica

Mary Wong: … the registries and the registrars and a lot of times we represent very widely different interests. Some of my members for example will say that certain policy decisions that we are taking are to get towards commercial interests and do not adequately protect noncommercial interests that are sometimes more intangible, like insuring freedom of expression and the protection of privacy.

Some of the issues we're talking about at this meeting, like the WHOIS verification? How do you verify registrant data? There are lots of privacy issues there and some of the interests of my members would be to have a very high level of privacy. But another group might say, "Well, we might have to sacrifice that higher level of privacy to ensure for example, greater access to the information by law enforcement and so forth." That's just one example.

So essentially we don't quite scream at one another, but our discussions are very, very rigorous, very, very passionate, but then what happens is after the meeting, we go off to dinner, we go off to the bar, we karaoke together at music night.

A very dedicated professional community and I have learned a lot from everyone. So I have greatly benefited from this community, from the support that ICANN and the staff have given to all of us who were all new at one time.

The last thing that Janice asked me to mention briefly before I take questions is the structure of the Non-Commercial Stakeholder Group. I've given you one example of times where the interests of some of my members might be very different from the interests of some of the other Stakeholder Groups.

As a Stakeholder Group, we are the framework for all the non-commercial users that would like to participate in GNSO policy. When we started, it was actually just one constituency, so it was almost as indistinguishable. It was a Non-Commercial Users Constituency, or NCUC - that's another acronym for you - and then we did a restructuring in the GNSO a few years ago, where the original registries' constituency became the Registry Stakeholder Group, registrars became the Registrars Stakeholder Group.

The Commercial Stakeholder Group is comprised of three constituencies - you may have heard from some of them. The ISPs form one, the Intellectual Properties Interest form a second, and the Business Constituency form the third.

In the Non-Commercial Stakeholder Group the NCUC transformed into the NCSG, but the reason why we wanted the SG structure or the Board wanted the SG structure was to bring more people into ICANN.

So very recently I think the third speaker you'll hear from today is one of the early members. The NCSG as a stakeholder group welcomed a new constituency, the Nonprofit Operational Concerns Constituency.

So what then happens for GNSO policy making is that, as a member of the counsel when I am asked to vote on certain motions and decisions, when we have discussions, I am there to represent the whole stakeholder group, not just the NCUC, and not just NPOC, the New Nonprofit Constituency. That can get very difficult, because sometimes even within each stakeholder group, if you've got more than one constituency, there can be differences of opinion.

So if you come to the council meetings you'll see us talking, voting, debating and like I said sometimes it gets a little passionate. But even before those public sessions you can attend either live or remotely, depending on whether we're doing here in the ICANN meeting, or in-between the various ICANN meetings.

Every group has its own regular policy meetings. We do, as a stakeholder group as well. If you come to some of those meetings you will see, again some very

vigorous debate within the stakeholder group before we can take a position, and before I vote on it at the council.

The one thing that I think that is unique about the noncommercial stakeholder group compared to some of the other stakeholder groups is that as a council member I am not necessarily bound by what my members say.

In other words our charter allows each counselor to vote per conscience. In practical effect my conscience means I do what my members tell me they want to, but it is a very interesting facet of ICANN that it is not a top-down management model, and I think the GNSO is a good representation of that.

Each of the stakeholder groups has its own charters. Each of our processes are different, but ultimately at the council we try and come to a good decision that we think is truly representative of the multi-stakeholder model, and in that respect I am happy to say that the NCSG is growing. We have over 200 members. Actually more now than NPOC has joined - that's more than some of the other groups, but we are very, very proud of the fact that compared to all the other stakeholder groups, our members are truly international a geographic diversity cannot be beaten by any other stakeholder group.

So I would like to welcome you all to ICANN. I know a couple of you were at the NCSG and NCUC meetings yesterday. A belated welcome to you and I invite you all to look at the ICANN website and to check when our next meetings are, listen in, get to know us. You'll find that we are as much a fun crew as the next person. So thank you very much and I'm happy to take questions.

Janice Douma Lange: Katie, why don't you start us off and remember to say who you are?

Katie Ann Davis: Good morning everyone. I am Katie Ann Davis from Jamaica and when the hours at the meeting yesterday and it was extremely exciting. I think I found my

niche in ICANN and I am willing to join that constituency. However, I looked at the structure and I noticed that there is no representation in the constituency for the Caribbean. I see North America and South America, but who represents the Caribbean?

Mary Wong: Thank you very much, and I remember you at the meeting. Thanks for participating. She spoke up at the meeting and made some excellent points and we are very happy that you were there. Your question relates to the council representation from the NCSG, correct? And you're right - there are representative from North America, from Europe and I am one of the two Asia Pacific representatives.

The reason for that is this - each stakeholder group is assigned by the framework, three elected council members. By our charter there has to be geographic diversity in that not all three, for example, can come North America, but as you know there are five geographic regions, so it's not possible for each election to have five different regions represented, but to the extent that different people from different regions run, it is in our charter that we have to ensure geographic diversity.

So if you for example not to single you out, although I really think I am were to join our constituency or the stakeholder group - I'm sorry we're still getting used to this new framework so it gets a little confusing even for us - and you wanted to run for the council and you got elected.

For example, I'm term limited out from after Toronto, so it may well be hypothetically that you would run and you would get on, and then we would then have a Caribbean rep, an Asia Pacific rep, a North American rep and so forth, actually maybe three out of five. So it's not an exclusion; it is simply the way it is structured. At any one time you would have maybe three out of five regions, but we hope to rotate such that we have all the reasons overall, most of the time.

Janice Douma Lange: This is Janice for the record. Marilyn Cade teaches us all very well. Two things; 1) It's amazing, Mary, that Paris was your first meeting. San Juan was my first in 2007 a year earlier and that you have been now on the council twice. Thank you for coming in and just acknowledging that when you walked in, you knew two people, and it is - it's daunting there were over 700 people at the Paris meeting and that's just extremely daunting.

And so we talked a little bit about that on Sunday how it feels like everyone knows everyone else; you're the only one that's not talking to anyone and then you can see what happens. You just need one or two people to take you in and that's the beauty of the Fellowship Program because you always have somebody to take you in, and everyone doesn't have that benefit and so we ask everyone and our friends from At-Large I have to say that has always been that way, bringing everybody into the fold and welcoming. So I think that was very important to say that. My question is why not the Intellectual Property Constituency for you? Hearing your background, I just wondered?

Mary Wong: I think that's an excellent question and before I answer that, I would like to emphasize what you said earlier. Having someone that's happy to take you around, there's always someone, but it really was intimidating and I'm just going to tell two short little vignettes of stories.

First is that when I went to the ICANN public forum, which will happen tomorrow afternoon. I don't know if your program allows you to go there - and that is one of the attractions for a lot of people have actually taken the time and the expense, and some people pay their own way. As you know most of us actually volunteer our time. So even though we're council members and our travel is paid for, the week off from work that we take, we don't get compensated for it either by ICANN, or by our workplace. I'll answer your question because sometimes what I do is much more closely related in my day job to what the IP entrants here do.

The story I'm going to tell is when I went to my first ICANN public forum in Paris, 1700 people, and people are talking to the Board and in a nice way I set to directly engage the Board that is one of the attractions. You stand there, you say your name for the record and you say, "I have an issue with ICANN," or "I would like to compliment the Board."

You can say whatever you like within whatever the topics have been set. I was very puzzled that the Chair of the Board, whom I would never have met in my life - he was not one of the two people I knew, and somebody would stand at the microphone and he would say, "Yes the next speaker at the microphone is X." I'm like how does he know X from 1700 people, and then Y and Z? So it seemed to me like a very insider community and I was scared.

The second story is when I first got on the council, which was I think was three months later was the next meeting - we were not as well organized in those days. Nowadays all council members have our names, and we ask those in the audience to at least let the council members sit at the table first. That wasn't the case in late 2008, 2009.

My first council meeting I sat at the back of the room, until they asked, "Well who is the new NC counselor," and I was like, "Me." I had met maybe less than half of the people on the council that I now have very good relationships with, so I just want to emphasize what Janice is saying.

Get to know people, because people are very, very helpful, but as to your question. I was an Intellectual Property attorney before I became a law professor, and a lot of the members of the IPC are actually professional colleagues and friends of mine, and we work together on a number of issues in a number of different forums, not just in ICANN.

There is a structure to the IP constituency that does allow individuals to join. I think the only reason why I'm not a member of the Intellectual Property Constituency is simply because members of the Non-Commercial Group reached out to me and I felt personally that a lot of the interests that they were

representing in ICANN and I am going to be very candid with you, were underrepresented.

The domain name industry has changed; it's growing a lot. A lot of people have built businesses and business models based on the industry, based on ICANN's decisions and we feel in our group very committed. I said to the multi-stakeholder bottom-up consensus building model. And in order to have that reality, you have to have everybody in the room, not just government, not just commercial interest, but noncommercial interest I said earlier, sometimes to people it's a little diffused, it's a little abstract.

You want to talk about human rights of the internet at ICANN when we're technically managers of the internet system? That's where I felt the most empathy and yet when I've been here, I think one of the things that hopefully I'm happy to say that I've done is to work together with other constituencies, including Intellectual Property Constituency where sometimes there are differences of opinion, but sometimes we have also stood together and made joint statements to the ICANN Board.

Janice Douma Lange: Well done. We need to move on to John and his presentation, so again I want to thank you so much, Mary - that was perfect. I couldn't have asked for anything more, great journey, great story. And as you can see John has got his presentation up and ready started. Do you need me to load that one up?

John Crain: Good morning. My name is John Crain. I've been at ICANN forever. This week my title is Senior Director of Security, Stability and Resiliency. I don't know what that means, but it's a really cool long title. First things first, who got up and sang last night? None of you, okay so one of the things you're here for is of course to interact with everybody. So I'm just seeing how many of you are actually getting up there and partying.

So ICANN has a mandate that starts with a bunch of Bylaws. If you're a lawyer and you like to read Bylaws, you'll see that the very first Bylaw that ICANN has talks about the security and stability of the domain name system, or actually the identifier systems.

So, when people talk about ICANN, they talk about the domain name system, but there are hundreds of other types of identifiers that ICANN and IANA is involved in. We have ones that are obvious or of course IP addresses IPv6 addresses. So it's the security resiliency stability of all those identifiers, it's not just the main names. The main names are just the ones the people think of sexy and they like to talk about a lot.

So in the earliest days of ICANN around the turn of the century in the early days of ICANN there was one security person. He was also the engineer, the guy who went out and spoke, the guy who changed the milk in the refrigerator. We were about five or six people at ICANN at that time, and although we had security and stability in our mandates, we had about probably ten hours of staff time a week to worry about that, and that was one of my jobs.

Today just in our security group, we have six full-time staff. Not only has a lot changed in the way we see things out in the ICANN meetings, but when you talk about the ICANN secretariat, or the staff, we've also changed a lot, so we now have six people focusing on security. So, people always ask us what we do.

So mainly we look at systemic threat, so threats to the identifier infrastructure that threaten the system. So we don't look at somebody stole one domain name. Somebody stealing a domain name is not a systemic threat. It's annoying and the people whose domain name it is, it's very important for them, but it's not systemic to the system.

When we have organizations out there that are doing this on a massive scale - that means that people can't rely on their names, etc. and we're seeing methodologies of going after registrars, or registries - those are systemic; they are actually going after the system. They're not picking on individual users or identifiers. So that's what we focus on.

A lot of people worry about cybercrime etc., and so do we as it affects the trust in the system, but we're not law enforcement. We're just a bunch of security geeks, worrying about identifiers. We actually talk a lot to law enforcement, because we don't know much about what they do, and they know even less about what we do a lot of times. So we do collaborate mainly on an education base.

So what could a systemic threat look like? Has anybody here heard of Conficker? A few people; okay. So Conficker is a worm, a virus, a piece of code that, just like many of the other worms and viruses out there, imbeds itself on your machine and basically takes control of your machine; allows somebody else to use your machine to do whatever they want. Normally they don't do this to do nice things, and normally they'll be trying to steal your data, or that using is part of distributed denial of service attacks.

What was interesting about Conficker is the way the way the bad guys controlled their network. They have millions of these machines - and I do mean millions - and the way they controlled it was by using domain names, and the way they were lining up these domain names, because every time a bad guys gets a domain name, we try and take it off of them, or law enforcement tries to take it off of them. What they were doing is they were generating lists of names every day. So every day in the beginning it would have been 200 names. By the latest version it was up to 50,000 names every day. And they were generating these in some secret automatic method, that's what they thought, so that they could basically stop the good guys from preventing them from using their network.

That's systemic when you've got 50,000 names a day being used for malicious activity - that's not a good thing. And people actually writing code to misuse the identifier systems - we decided that was a problem. We were approached by private industry and law enforcement on an international scale saying, "Help. We don't know how to talk to these people in the internet industry."

So that was where ICANN came in as a coordinating body. We basically talked to all the TLD operators that were involved - it was 110 countries that we had to talk to - we had 21 days to do this in, and we basically distributed knowledge to these people so that they could help combat this. So that's a systemic threat and needed a systemic reply.

To actually tackle that threat also the system has got to fight back, so that's the kind of thing we were looking at. We also look at other systemic threats - the widespread registration of nefarious names. So if there's a lot of names following a patent being registered, then we're interested in that. We may not be able to do anything about it, but we might be able to educate; we might be able to help law enforcement talk to people, or the registrars talk to people. So we tend to be a bit of a middleman.

It's very easy to subvert DNS, so one of the things that we look at is protocol weaknesses. Has anybody heard of DNSSEC? Actually it's not really a new protocol of such; it's an addition to existing protocols.

Can you believe that for over 20 years we've been using one of our main protocols and it's not authenticated? You cannot actually know that the answer you get is the answer you were meant to get. Most of the protocols were designed 20 or more years ago. They weren't designed for people to actually come on the internet and use it.

It was engineers, university people. It wasn't my mother doing her email, or doing her banking. Nobody really thought of that apart from a few science fiction writers - maybe Vint Cerf and a couple of other people thought that would happen, but most people didn't. So the protocols weren't designed with security in mind. And in fact it wasn't until the late, or the mid-1990s that you had to include security as a thought in a protocol document. So today if you write what we call an RSA, or a protocol document, there must be a section called security, and you must think about security.

So as you look at new protocols, for example SIP, which is one of the voice-over IP protocols, has a security section. Well, DNSSEC is, of course all about

security so it has a very big security section and all new protocols as they come have to take security into account.

The old protocols didn't do that, so protocol weaknesses are an issue, so we worry about those. So we work with the ITF under the bodies that are working on standards and protocols to see where we can help a little bit fix. I mean this is not something ICANN can fix, right, this is protocol work, this is deep geek. This is about as geeky as you can get. We have a few geeks; some people say I am one. I deny it; I'm the cool one apparently. So this is really in-depth stuff. Now if you mix with the crowd at ICANN, which I hope you'll do, you'll see that there's actually some extremely smart protocol people here.

If you look at the Security Stability Advisory Committee, half of those people on that committee are people who go to things like ITFs and work on protocols. They're very deep into the protocol, and if you're going to have a secure and stable identifier system, then you must be in the protocol space as well. So we interact very closely with the entire engineering task force or thee ITF to worry about protocols.

The other thing that we do, and we do a lot of, is training programs. You might think well, what's training got to do with security? And the answer is everything. If you want to build stable secure systems, you have to be trained. So we've trained over the years, I've been doing these training programs for about seven years now, hundreds of staff from ccTLDs mainly. So we can give training pretty much anywhere on the planet. They're free trainings, that's one of the things we do, one of the things that ICANN can bring to bear as we can fund those trainings. We do have skills sets in-house to train, but we don't have 20 or 30 trainers, so we work with partners and we collaborate with organizations like LACTLD, AFTLD, all the other TLD organizations. We work with an organization called the Network Starter Resource Center, that also do a lot of training and development.

The basic idea of the training program is to bring up the level of knowledge. So these can be technical trainings, they can be business process trainings. So one

of the trainings we do is in Disaster Management. It's not just security, it's also stability and resiliency, so you need to do Disaster Management.

So all the TLDs, we go out and tell them this, you need to do this - this is how we do it and then we bring in experts to give the trainings. So we spend a lot of time on training, so if you're involved in the ccTLD, and you think it's training that's useful, come talk to me. We may have a program, and if we don't have a program, we may be able to find you one, or we may be able to develop one if there's enough interest.

Seven years ago the only training we did was how do you turn on a DNS server. Very simple technical trainings. Today we do trainings on, as I said disaster recovery, but also securing networks, monitoring networks, more advanced network topology. There are a lot of things that we can help the ccTLDs and the other TLDs, and sometimes registrars come.

So people in the community of managing the infrastructure, we can help to make sure that they have a reasonable level of knowledge about security, stability and resiliency issues in that business, because generally they're all businesses. Those are the main things we do. We do lots of other things, but I'd be here until tomorrow and I wanted to talk about one of my pet projects in a minute. First I'd like to ask if there are any questions about what we as a group do, or ICANN in security.

Male: Actually I have three questions, one related to DNSSEC. Is DNSSEC implies EDB, or TCP protocol? DNSSEC where there are complications between the domain space, so it's using UDB authenticity protocol…

John Crain: So I've got security in my badge title, not engineer, but I know a little about engineering. So it can use both, just like regular DNS. It uses something called EDNS-0, which allows you to use larger UDP packets. So one of the problems that both IP Version 6, and DNSSEC face is that a lot of middleware, firewalls,

etc., have - I'm trying to think of a nice way to say this - that they weren't quite thinking when they developed their code.

So they have parameters in there like do not allow anything over 512 bytes if it's UDP. Now of course IPv6 does things like MTU discovery and it can have much larger UDP fragments and DNSSEC is the same. So sometimes you do revert to TCP with DNSSEC. So there is a misunderstanding often out there that DNS is a UDP protocol - that is incorrect. There are always a small percentage of queries that will be TCP based. On the root server that I'm involved in, we see a very small, and I mean very, like sort of less than 1% of TCP traffic. So DNS is both.

Male: Second question is related to one that could… (Inaudible) initiated from the resolver on DNS, either on the DNS and local DNS or ISP DNS. It assumes that if no resolution for the domain name during the cache on the way to the server. So the request will send them to the server. What is the time of authentication between the local resolver of the DNS and the root server on the DNSSEC?

John Crain: I think I know what you're asking here. I should probably give a different presentation after this. So root servers are what we call Authoritative Servers and they only answer for questions that… you know when they give an answer, they will only tell you about top level domain. So typically - I normally do this with a graphic, and I don't have it handy, so I'm just going to try and run through it - typically when you as a user do a DNS query, you have a server that sits at your internet service provider or your business. That's called a recursive server. What that means is that it's going to go out and ask questions, and keep asking questions of different places until it gets you the right answer and then it will answer you.

So what will happen, is it will go to that recursive server and it says, "Do you know about www.ICANN.org?" And it may not, if it's a brand new server,

never used -it will actually know nothing. The only thing it will know is the address of the 13 root servers, so it will go to one of those root servers and it will say, "Do you know www.ICANN.org?"

Male: Here the question actually; this is the point of the question. Okay right now that is (inaudible) the 13 servers, okay - he has (inaudible) server, so as a DNS request will forward one of that 13 to delegate to .com or .org or whatever pertaining to any of the TLDs. Okay, here's the question - how do the root server authenticate that query message, because I know, you can correct me if I'm wrong, there is an indication between the root server and underlying server for example all the TLDs, but the request from ISP itself.

John Crain: Okay, let me go through the process and then I think it will answer it. So that recursive server will get an answer from one of the 13 root servers and there are different randomization methods of choosing which root server. It sends back an answer and it says, "Here's the name servers of .org." That machine will then cache that information, and then it will go on those name servers, "What do you know about www.ICANN.org?" And those servers will say, "Well we don't know about that machine, but we know about ICANN.org." That information will come back, be cached, and then it will go off to ICANN's DNS servers, and we will answer with an IP address, right. So you've now got the IP address, but in the caching, you have a lot more information.

So now I want to go to www.ITF.org. I ask the question as an ISP; I don't ask the root server. I know .org, so I go off to .org. If I came and I said, "Show me ntp.ICANN.org," I would ask my recursive, and my recursives would say, "Well I already know ICANN.org," so I won't even ask .org. I'd just go straight there, so the caching basically allows you to cut down the amount of traffic.

So, a typical root server like the one we operate sees very few queries. We only see in the range of 10 to 20,000 queries of seconds; whereas something like .com or .org, or .net, or a ccTLD will see orders of magnitude larger than that, because they have much bigger zones. I don't know if that answers.

Male: I got that answer.

Janice Douma Lange: I'm just gonna say, too, in bottom-up, if this is going like this, over some heads, you know, do not be afraid; it happens to all of us. And remember what Mary is saying, this isn't all a technical community, but we are part of that. But the other parts of it, the noncommercial parts and everything, so you're still in the right place. You're just hearing language that's a little strange to you and you don't have to take it all in, but I think if anyone went to DNSSEC for beginners; a little bit of this kind of clicks in about going back and forth to the servers and such, but you know, don't worry, just keep sponging it in as you can and block it if it gets too overwhelming. Mary.

Mary Wong: I was going to say something similar, but I don't have a technical background, I still don't and a lot of the things that John does would be completely in worse than a foreign language for me. But over the time that I have been involved with ICANN I started learning some of the things at least at somewhat a superficial level. And as Janice says, if you go to the workshops and things you do get more familiar with things. There are times that I do kind of go, "Oh wait I think I know that, but I'm not sure what that means," and I go and ask somebody, but over time it did get a bit easier for me.

John Crain: Yeah, and the other thing to remember on that is that as engineers we also don't know what lawyers do. You know, it's a completely foreign language to us. The good news, if you're not an engineer, and you don't have a technical background is that once you start grasping the basics, the DNS is an extremely simple protocol. So it won't take you long to sort of ramp up and learn about it. So we have another question.

Fatima Cambronero: Hi, I'm Fatima. I am a lawyer, but I have a technical question. You said recursive were coming for DNSSEC. What is the number? Maybe you can explain what the recursive is?

John Crain: I actually don't know the numbers off the top of my head. So, it's not governments, DNS owns a recursive signed by the administrators and they're not always government. Sometimes they are and sometimes they're not. You know ccTLDs are managed.

So the real question is; how many ccTLDs have been signed. Not as many as we'd like. We do know that about 80% of the existing names can be signed, but are not signed, and it's only about 2% of the names that are signed. So it's still a very small percentage, but it's not 80% of the ccTLDs or the TLDs for example, because much of the name spaces is in generics, and most of those are signed. So it's getting there, it's very slow. The chicken and egg problem with the DNSSEC is about getting things signed, getting things to be able to use that, but it's not a large portion, but we're seeing more and more every day.

We're giving trainings to the [C study] operators and we're getting a lot of requests for training. So there's a lot of interest. One of the things that I always push when I'm giving these trainings or when we're developing these trainings is to get them to a situation - the operators - that they can make a well informed decision, about whether they should sign, how they should sign, so we don't really push them to sign. It's their infrastructure, their systems. They are the ones that got to decide, but it's growing, but it's not like everybody signed, definitely not.

Janice Douma Lange: Yes, there is one question from a remote participant, Waqar Azeem from Pakistan. He is interested… you were thinking about the trainings. He is interested. Are these trainings open to all, or is this for specific people? The

second question - who handled the root servers technically - your team or some third party? Thank you.

John Crain: Okay so the trainings are aimed really at people who operate infrastructure, internet infrastructure, I don't mean commercialized, it's not aimed at commercial organizations. So if you've worked with, or were associated with a ccTLD, then that's a definite, you're always welcome.

If you work in a registrar and you're in the neighborhood, we never say no, because we want to get everybody trained, but the programs are aimed at ccTLDs. We're not very strict about not letting other people in, because if people want to learn, and it helps increase the stability or the security in the system, then we're very open. If you see a program in your area and you're not sure, then ask. If you don't ask, the default answer is no, right, because you've not asked. So if you don't know ask, because you never know, you might get a yes.

Operation of the root servers - so there were 13 root servers operated by 12 organizations. ICANN operates one of those root servers, you're all sitting there thinking so who operates two. It's VeriSign, they operate ANJ, so there are 12 organizations, and if you go to our websites, and I'll say this slowly, I don't know if you can tie this in Janice to the remote participations. It's www.root-servers.org, and that's a site where we put in information, all the operators put in information for the public about where we have locations exactly. Actually my next presentation is going to talk a little bit to some of the measurements around root servers.

Janice Douma Lange: Just a last question from a remote participant to cover them. How end users are affected by incorrect implementation of DNSSEC by TLDs? This is from the same person, Waqar from Pakistan.

John Crain: So it's no difference really to incorrect implementation of any of the protocols. If you do it badly, things break. So that's why I say all of our trainings are aimed at making to make the right decisions. There is some intricacy to DNSSEC that is not in the regular DNS. In the regular DNS, lots of things break all the time and it still kind of works, and DNSSEC is less forgiving. So your engineering principles need to be solid. That's no different really, to many other things when you're running businesses, if your engineering principles aren't solid than things fail.

We've seen some interesting issues around key failures and things in the batteries and even in the live environment, but so far nothing really disastrous has happened. And if you look at the root signing, which we are responsible for, you will see that we have extremely elaborate procedures and guidelines and checks to make sure that nothing goes wrong.

I would recommend that you go to our website and look at some of the DNS operations stuff that we do, and we try to set a standard and that standard is very high. Go look at that and see the kind of things that people are doing, or maybe go and look at some of the other countries that have signed and see what they're doing, and you'll see there is a lot of process involved in being very careful. You should do that with all of your engineering, and in some ways DNSSEC isn't really any different from other engineering things.

Simon Balthazar: Simon Balthazar from Tazania. First of all I want to congratulate you and your team for the training that you've been conducting all over the world, especially in Africa, for us, mostly TLDs, we've really gained a lot from that through STLD. Second of all there have been quite a number of DNSSEC platforms from different organizations that are trying to help us, mostly TLDs to deploy DNSSEC, just to keep up with the speed of the internet. What is your view of these in terms of knowledge spread and…

John Crain: Do you mean technical platforms or do you mean technical platforms?

Simon Balthazar: Technical platforms, like a PCH, and Afilias.

John Crain: There are a lot of people that are out there training and they all have the same thing in mind. At the moment we have unauthenticated DNS, and we all see DNSSEC as a solution to that. So I mean, I know the trainings from all these people. They are all good quality; they all tend to have the same goal. You have to remember if you go to a more commercial organization, they're going to have more commercial interests at the end of the training. What we set ours up for, so we set this up, not for the people who can afford to go out and get commercial training; we set all our trainings up for those people who can't.

So the training we do is very non-commercial. Actually we've had people from those organizations that do the other trainings come and give our trainings, so we work very closely together. I mean from the quality of the materials, they are all excellent. I would say if you get an opportunity to get some free training, or very cheap training for a DNSSEC, from any of those, you should go for it, because they're all good, at least the ones you mentioned. There might be others out there that I don't know, but the ones you mentioned and a few others that I can think of all do outstanding jobs.

Gabby Gijon: Hello John, hi everybody I'm Gabby Gijon from Argentina. I'm an engineer and I'm so interested in network security and information security specifically. I have two questions, John. Does you work align with any security standard, like ISO? What about the use of [Brink] management methodology?

John Crain: So, we don't certify to a standards because that costs a lot of money, but we follow some of the ISO standards, and because much of what we do is based in the US. We follow NIST standards which are very much aligned with ISO standards, and what we find is that those standards are extremely large and complex. So, we try and break down the pieces that are really relevant to it.

The Brink stuff, we do some of that too. We are still, even with six people in our infancy when it comes to what I call info sec, like IT security so we focus a lot on the protocols. We also focus of course internally; we run a network, so that's where we do a lot of the standardization and of course for the signing, etc. We still got a way to go.

The problem with security - and anybody who's an executive here at a company will know - that it's this mystic thing that is very hard to spend money on, because it's like an insurance policy. Everybody says, "Well my car will never get hit by lightning." We invest an enormous amount into security, but we could always invest more - that's not just in processes, but also in everything around info sec.

But I'm happy to talk to you offline about more in detail about what we do. We're on a thing, so I'm not going to go into too much detail over the microphone, but I'm quite happy to go and talk to you and introduce you to some of our security team if you'd like. We are by the way, we have four of our security team are actually here and you can approach us all. We look a little bit rough and mean, but we're not. We're nice people, maybe I'm not, but the rest are very nice too.

Gabby Gijon: One question more by curiosity. Did you work with root servers when happened the DNS attack in 200…?

John Crain: The answer is yes, whichever one it was, yes.

Gabby Gijon: The reveals the need of implementing the basic…

John Crain: Some of the things I can't talk about for root servers. Security is always this awkward thing where, when you're being recorded and you're live on the internet you don't really want to talk about too much detail. But I can tell you that, for example, root server operators get together on a regular basis, exercise, do table tops - all the things you would expect them to do. You know, we have elaborate out of bounds communication, and inbound communication systems, much more so than people expect.

Often people say, well the root servers is just 12 different organizations. We meet at least three times a year to discuss all these kind of issues. We test everything we do constantly. My phone could go off any second and it will just be a test and it's regular. So things like the DDoS and especially when they become public knowledge and they put political pressure, that's how it works, which is why they put pressure on your executives, have over the years put us into a situation where we are miles ahead of where we were in 2007, and in 2007 we were miles ahead of where we were in 2005, and in 2015 we will be miles ahead of where we are today, and you know DDoSs happen all the time against the root servers, you just don't see them. There was one in 2007 and I believe one in 2002 or 2001, and those were visible, so those are the two you hear about. There's been much bigger ones than those since then that you don't hear about.

Janice Douma Lange: John, I think we should move to the second half of your presentation.

John Crain: Yes, if we still have got time.

Janice Douma Lange: Yes, we do, and while you put those slides up and Siranush does, I just want Veni to introduce himself, because the group hasn't met you yet and they need to leave.

Veni Markovski: Thank you I am Veni Markovski. I'm responsible for the Russia, former Soviet Union, Eastern Europe, and some other countries, which keep on showing up on the map in this part of the world. I've been with ICANN for quite a while, I was on the Board, I was seduced by the Doc site and worked for the staff, but if you have any questions in this part of the world - and I see here there are several people from the region feel - free to approach me thank you.

Janice Douma Lange: Okay Veni, thank you. Are we set for remote? The Atlas too? You've got that up, the second one?

John Crain: While they're getting the slides up, I'm going to point out that this is not an ICANN project. It's just one of the toys I like to play with on the internet. It's something I'm supporting and I'm hoping you're going to help me support in some way, and I'll talk to that in a little bit, and it's a measurement platform that we're going to talk about and actually that's the last slide so I'll go back to the beginning.

Are we good on the slides? We're good. Okay, so how many here have heard of Atlas in the framework of measurement? Nobody, that's exactly what I expected, oh one person, the person who also went to the trainings and things. That doesn't surprise me. There's a few of us that were enthusiastic about this. So Ripe Atlas is a basically, I'd like to think of it as a community activity that's designed or managed by the Ripe NCC. They're an organization in Amsterdam that distribute IP addresses, but they also have other laboratory if you'd like.

One of the things they like to do is measure things. Coincidentally the Ripe NCC also manages one of the 13 root servers, so they're one of those 12 organizations. What they're trying to do is build maps - maps of the internet, or measurements of the internet that actually overlap onto geographic maps and they are trying to measure in real time. So they're not collecting data and then analyzing it like two months later, or doing anything very passive. They are doing what we call active measurements.

They are actually sending out queries using some very small probes about this small, those of you online, of course, can't see this, but it's about the size of one of these dongles; I don't know what you'd say that was the size of it. It's pretty small, maybe it's like a D size battery. What these do is they send packets, which are normally DNS queries to infrastructure. So they send a lot of DNS queries to root servers. So typically, when you've done these kinds of measurements, there's a tool called DNSMON also from Ripe NCC that may have 20 or 30, or if you're looking maybe a hundred points in the network from where they measure.

So we had a discussion in Atlanta, Georgia by phone, then chaired the symposium that was looking at risks to the identifier system, and one of the things that came out of that symposium was that we really didn't have any way to measure the network from the edge.

It's really easy to measure from internet exchange points and large providers, because you can get things into their infrastructure. It's really hard to get measurements from the edge. Unless you're doing something like settee, which was actually not really about measurement, but about calculating, but you've got code on people's machine. Thing is somebody worries about security, the idea of managing code that we put on people's machine didn't really appeal to me, because you know, there's always a question of how long will you own that code before the bad guys do.

The idea was to go with a hardware concept, and the idea is to use thousands of these probes in the long run. There's over a thousand probes at the moment. I

don't know if you can see that, I know I can't, but it's because I don't have my glasses on. There's actually about 1,400 probes live and in action around the globe and as you can see they're mainly concentrated in European theatre because that's where Ripe NCC is, but they are also on every continent. I want to see more of these out there.

So why would we do this? Well, if you can measure from thousands of locations, you just get this broader view and it gives you visibility into things that you otherwise cannot see. There are a lot of things you can't see from an internet exchange point, or from a root server.

We can see a lot of data on our root server about who is querying us, but that's what it looks like from our side, not what it looks like from their side. We're a service, so it's more important how it looks from their side than from ours, right. If they send us a query we answer, we don't know if they got it back. Just because it's a UDP kind of thing most of the time, so it gives us a view much closer to the user perspective.

Some of the things that we can measure, for example, are how fast can we resolve a DNS query - a standardized DNS query, because we're trying to be a little bit scientific - to the root servers. On each of these flags is a probe and you can actually click on these probes and dig in a little further. If you're actually hosting one of these probes, you can actually see all kinds of data about your own network as well, and this basically tells us where we should probably be putting root servers.

We've never had any data like this before, from where is it slow to get to a root server? We don't know, right, we're the root server, but we don't see how long it takes for the answer to get back. This is telling us that. When we deploy what we call any cache or distributed DNS - I'm being candid here - we're typically guessing as to where to put these things. Some things are very intuitive, you know there's an IXP over their internet exchange point, let's put one there, but is it the right internet exchange point? We don't know, so this is giving us insight

into things that we've never really seen before, and I like that because I'm a geek and I like data and I like real data.

So the basic idea is that you put one of these on a network somewhere. This USB thing on the other end, that is not for data; that is just for power. No data goes over the USB, so I can happily plug it into my laptop and nobody can see my traffic. I've got a special one for some people that I don't… so nobody can see traffic. The other end of it basically goes to a cap 5 cable, DHCP gets an IP address, loads its core software.

There's a whole computer in this, everything you need to do this is just in its little box; it's fascinating. This card originally was designed for managing vending machines remotely. Imagine you've got a few thousand vending machines out there and you want to count how many colas are in there - that's what the card was all about, and some smart people at the NCC thought. "Oh, that would be cool. We could do something good with that," and they put it into this nice pretty housing and found a new way of powering it instead of a motherboard and made this. So not only is it good, it's cool and it's geeky. So if you can show your friends you've got one of these, you can be a real geek.

So if you've got one in your network - so I have one at my house - I have some security systems hidden away somewhere and that just happens to have a USB and network, so I just plugged it in there. At one time I had it plugged into the back of a hard drive with this going to my DSL router. Pretty much anywhere where you can get DHCP, which is the protocol that gives you the IP address. If you're not technical, if you have a wireless router at home and it has cap 5 or network cable on the back and it has a spare port, chances are you can run one of these.

So this is measurement from my home to L-root server, because L-root server is the one that we run, so I just decided I'd show that one. I could have shown any of the other root servers. I can see them all, and it tells me how fast I can get there. Well, if you're not a geek, then that's probably not exciting.

I can also look at the map and see if my network is up. I get a little green flag on the map above my house. If my network is up and a red one, if it's not, you don't need to be a geek to find that useful. My wife finds me and says, "The network is down," and I look on there and I say, "No it's not. It must be another issue." So, there's all kinds of things you can use them for. But what the real purpose is, is to get a better insight into the infrastructure.

At the moment, it's just root servers, but there's no reason why you couldn't do this for a TLD, or whatever, and if you're running one of these at your house, they are starting a new project which will allow you to do some queries yourself. So you could say sets yours to query your name server and you get some other ones to query your name server, so there's more and more things you can do with it.

So what do you need to do to host one of these things? What do you actually need to do technically? You need some kind of always on connection. If you're connection is up and down every five minutes, the people from the Ripe NCC get very annoyed, because it doesn't give them very good traffic apart from the fact that your network is up and down every five minutes. Always on – that's DSL, cable, it could be satellite, whatever it is, that it is always on.

USB power, a lot of routers have USB power. If you have a machine, it has USB power. Any USB port typically has 5-volts, and that's what it is. We have a lot of things that we use for powering things. I'm just going to actually garb one of these, because I'd be shocked if I didn't have a USB power in my bag. There you go, there's a USB power.

Anybody have a telephone that uses USB to power? You have an iPhone, an iPad? Many of the other tablets and phones - they use USBs to recharge, well that's a USB power. So if you just have one of these lying around the house you have USB power, so that's the easy one. That's why we designed it with USB power, because it's everywhere and it's always the same voltage. It might be different wattage, but it's 5-volt everywhere you go, so you don't have to worry

about 110 volt, 120, 230, different plug types; we just say get USB, so that works.

A cap five internet connection - what I mean by that is cap five is some kind of router at home. If you have a wireless unit at home, chances are you have a cap five on the back. If you have a remote hard drive that is connected, some of those have cap five on the back. There's lots of ways of doing this, even some keyboards these days have cap five that you can plug-in. It's amazing where they put that stuff.

DHCP, because we have to get an IP address to this, so it can talk to the internet and the last and most important thing is enthusiasm. So, if anybody is enthusiastic about joining a project like this, I'm happy to get you on to the project, give you a device to take home and let you join the project. But if you're not enthusiastic, please don't, because these are not cheap, and when I say not cheap, I mean not cheap.

If you're interested, the other thing you need to do is just come talk to me, and I think I have enough for pretty much all the Fellows, if everybody is interested. If you're not interested than please don't come talk to me, unless it's like, "Hey, can I buy you a beer," or something like that, than you can come talk to me too. So here's the URL and do you have any questions about that?

Janice Douma Lange: I will be giving you the presentation. The remotes, Siranush, if you can just make a note of the folks that were on today, that would like to have a presentation. We'll do that too, so you don't need to memorize the URL. And any questions for John, and let me just say if anyone wants to join us with John, you don't need to follow him out of the room. We have one more speaker here for us. I'll make sure that everybody has John's email address and that you can get him sometime this week.

John Crain: Or just give me a business card and I'll come to you. For those of you who are not in the room, if you go to that URL you can request a node. So if you hear somebody say, "Wow that's cool," which it is by the way, and you want one of these, then go to that URL and request one. Especially if you're in a remote location, the remoter you are the more chance you are that they will send you one, because they've got 5,000 of these in London, and they don't need any more there, they need them in other places. So do send them in an email, and if they don't send you one, send me an email and I'll see what I can do.

Janice Douma Lange: John, I'm going to say that if there are any questions please send them to me and I'll make sure that they get to John, because I'd like Alain to have a couple of minutes to speak to you here about NPOC, before we turn the room over to the GAC, okay. So thank you very much, John.

Alain Berranger: Good morning my name is Alain. I'm not leaving the room I'm coming around here. I must apologize to my Spanish speakers, because I love Spanish, but my level of Spanish is insufficient. I have 10-minutes with you to talk about how I came to ICANN and five minutes to tell you about NPOC. [speaks French] How many people speak French here? Bonjour l'Afrique. Arabic?

How many of you think they know a lot about the internet, so you can put your hands up? I'm going to be playing this game, so if I know a lot about the internet I'm going to put my hand up, okay? So who knows a lot about the internet here? Great, and so-so? A little knowledge about the internet, okay. No knowledge about the internet, really?

Alright, I came to ICANN because I was retired from International Development. I had some time on my hand, although my wife does not believe it, and I had some friends in ICANN who said, "This is really interesting and fun, and international, and why don't you give it a try?"

So I did, and then I discovered that I, you know, it took me weeks to realize that I wasn't progressing in my understanding. It was too complex, and I started talking to my friends and they said, "No, no, no, we're all are in that same boat." Just be like all the others, jump in and now it's been a year and a half. I'm starting to feel a little bit comfortable about a few subjects. So that's how I came to ICANN. I like it, but I've been in international developer all my life, [speaking French], for our friends of Africa, I spent five years in Africa and really, I travel a lot. I carry this in my blood internationalization. I love relations among people, and as a matter of fact I found these at ICANN - not as much as I wanted, but I became interested in the new constituency, the NPOC, but it's the latest baby constituency. We're the smallest, we're the youngest, and our idea was that we would promote the welcoming of not-for-profit NGOs in ICANN.

I observed that in a multi-stakeholders process, private sector, government, and civil society that really, we civil society, I say we, because I'm on the Board of a number of NGOs, that we were under represented. We were not underappreciated, we were just under represented, and that is my passion right now, my ICANN passion. I have many other passions.

My ICANN passion is to try to contribute to the internationalization of ICANN from the bottom up, by having more members of ICANN from developing countries around the world. I think that's going to be very good for ICANN, because you cannot have that bottom up process, and truly be global if you're not in Somalia, Bhutan and Peru, and everywhere else in the world. I have some basic material for newcomers, because we had a meeting with Costa Rican NGOs yesterday, so I'm using the same material. It's very simple material. What is ICANN? What is NPOC? Mission, values, objectives, so I'm not going to bother you with this now. You can read it.

We're still young in the sense that our website www.NPOC.org is really old technology, so we are going move away from that and go to a website, so that's why I'm distributing paper right now, and we would like to have you in our stakeholders group. The non-commercial stakeholders group and little

competition in between us I would prefer you join NPOC, but you take a look at what we do, what we plan to do and you decide.

I have membership forms that I left with Janice in Spanish, French and English. If you have any questions, talk to me, or else drop me an email. I think that's good enough Janice, or do I have time to take a few questions?

Janice Douma Lange: If there are an questions, we would have time for one or two, before we pack up, and again if you just need to think about questions, you can send them to me, and Alain and I are going to be at a finance meeting together at 9:30, so we'll be seeing each other quite a bit to do that, but if there are any questions just right away, we could take it.

No remote, then good. Alain, thank you very much this starts the newest constituency group here, which is so important that our Fellows understand the growth within the ICANN multi-stakeholders structure, and that there is an opportunity always for a voice that is not now heard to charter to come into the multi-stakeholder environment to be heard, so thank you very much.

For the Fellows, please as we leave, just come outside the door with me very quickly, and if you could just clean up if you have any coffee cups, or anything around you so that we leave it nice and tidy for our GAC representatives here to start their morning.

And you know to the folks from the GAC that are coming in and have been here, I just want to say thank you for sharing this room. I know the space is available all week for all of ICANN to use all the different rooms, but we in the Fellowship Program so appreciate the fact that we can be here and enjoy translation for all of us as we start our learning curve in ICANN, and we really appreciate having this room in front of you for the day. So have a good day everyone, and for the Fellows, I'll meet you right outside.

[End of Transcript]