GISELLA GRUBER: Good morning, good afternoon, and good evening to everyone. Welcome to this At-Large Capacity Building Program 2015 webinar on the topic of Security & Stability. This is the seventh webinar in this program held today on Wednesday, the 10th of June at 21:00 UTC.

We will not be doing a roll call for this webinar. However, we would like to remind everyone to please state your names when speaking not only for transcript purposes, but also to allow our interpreters on the French and Spanish channel to identify you. Also, if I could ask you to speak at a reasonable speed to allow for accurate interpretation. Thank you very much, and over to you, Alan.

ALAN GREENBERG: Thank you very much for the record and interpretation. My name is not Tijani Ben Jemaa, but I am replacing Tijani today who couldn't be here. Tijani is the person who has organized these capacity building webinars, and for that I think we all owe him a debt of gratitude. I have the easy job after he's done all the hard work of simply saying that this is one of the webinars that I would have attended even if I wasn't supposed to be attending them because I think security and stability obviously of the DNS is obviously a critical issue, but it's also worked on by some of the more interesting people that we meet on these kinds of webinars. A personal statement.

I'd like to turn it over to Julie Hammer, who is the ALAC liaison to the Security & Stability Advisory Committee and our own star in this area. Julie, it's all yours.

JULIE HAMMER: Thank you, Alan. A little exaggeration, but I thank you very much. Next slide, please. What I would like to do in the seminar today is touch on some definitions, discuss ICANN's role, talk about why security and stability is important and then cover the role of the Security and Stability Advisory Committee (the SSAC), and then I'm going to be handing over to Dave Piscitello and Richard Lamb from ICANN staff who will talk about some very interesting details of ICANN's Capability Building Program as well as I'm sure any other interesting aspects of security and stability. Next slide, please.

Just two [inaudible] on what ICANN's mission is. It's to coordinate the allocation of the Internet unique identifier system, and importantly it's second listed technical mission is to preserve and enhance the stability, security, and resiliency of these systems. You can see another two role there: to maintain and operate the L-root name server [instances] to and for the community and to manage ICANN's own internal systems and to provide a public [play] accessible portal to disseminate and share information.

It's that second role, the security, stability, and resiliency of the systems that we're focusing on today. Next slide, please.

To try and define what we mean by that, I've extracted these definitions from the SSR framework. I'll just quickly read them. Security is the capacity to protect and prevent misuse of the Internet unique identifiers. Stability is the capacity to ensure that the system operates as expected and that users of the unique identifiers have confidence that it will. Resiliency is the capacity of the unique identifier system to effectively withstand or tolerate or survive malicious attacks and other disruptive events without interrupting or ceasing service. Next slide, please.

So in that context, it's important to understand what ICANN is not. I've listed a number of things here. ICANN is not a law enforcement agency, a court of law, or a government agency, although law enforcement and government do participate as stakeholders in ICANN's processes and in policy development.

ICANN is not responsible for policing the Internet or operationally combatting criminal behavior. It is not responsible for determining what constitutes illicit conduct on the Internet. It is not involved in use of the Internet related to cyber espionage or cyber war. And it's not authorized to unilaterally suspend or terminate domain names, although it is able to enforce its contracts with third parties including domain name registration providers. Next slide, please.

So that's what ICANN is not, but what ICANN does do is play a role in supporting the work of law enforcement or government agencies in carrying out their legitimate actions, and that is done on request.

It does participate in the operational security community in studying, analyzing, and identifying malicious use of the DNS, and it does play the same part of any interested stakeholder with regard to Internet protocols. More specifically, in the evolution of Internet protocols and related standards that are not under the purview of ICANN, but are actually developed in the Internet Engineering Task Force (the IETF) and the Internet Architecture Board (the IAB). Next slide, please.

So there are a number of ways in which we can consider securities viewed within ICANN. First of all, it's actually a core value for ICANN and that is in accordance with the Affirmation of Commitments. It's one of the four focus areas of the ICANN strategic plan. It's an overall thematic area coming right across the organization. It's an issue that's of concern to every stakeholder group.

Security is also a department within ICANN, a security team. Security is an essential element in all projects and activities that ICANN undertakes, and of course it is a key stakeholder group within ICANN and that is the Security & Stability Advisory Committee. Next slide, please.

Just to dwell briefly on why security and stability is important, firstly, it contributes to the stability of the global economic environment. The Internet is fundamental to economic wellbeing in every country today and the stability of the DNS system contributes to that.

It assists the prosperity of developing and developed nations. It supports national security, emergency response, and the preservation

of law and order. It facilitates the correct functioning of critical infrastructure and that role is growing, in my view, the degree to which critical infrastructure relies on the DNS for its function.

It enhances opportunities for business and commerce. It enables the free flow of information, and it protects the interests of individual users of the Internet. Next slide, please.

To just share a little information on the Security & Stability Advisory Committee (the SSAC), the SSAC's charter is to advice the ICANN community and the ICANN board on matters related to the security and stability of the Internet naming and address allocation system.

SSAC was initiated in 2001 and began operation in 2002, and it provides guidance to the board, to supporting organizations and advisory committees, to ICANN staff and to the general community. As of today there are 34 members of the SSAC, all of whom are appointed to the ICANN board for three-year terms. Next slide, please.

The SSAC activities are focused in a number of different groups. The membership committee is one of the permanent committees of the SSAC and it reviews how each SSAC member contributes to the group. There is quite a newly instituted permanent work party that actually tracks the advice that SSAC has provided to the board and what the outcomes of that advice are. There are work parties that plan the activities for ICANN meetings, both the SSAC private meetings, but also the DNSSEC workshops that are open to everybody and SSAC outreach to law enforcement.

The SSAC has an annual workshop for two to three days that happens usually in September in each year where it retreats and considers its work program and reviews and updates it. Then there are specific SSAC work parties that normally conclude in the production of an SSAC report. One that has just concluded within the lack week or so is the Public Suffix List and that report has just been posted on the SSAC reports webpage. There is an SSAC party looking at how credentials are managed, looking at producing best practices for the protection of registrants and the credential management lifecycle.

There is the work party looking at where we're at with new gTLDs and what might need to be undertaken before the next round of new gTLDs, and there is a work party looking at producing a report from the 2014 Internet Governance Forum. Next.

The next three slides, which I will just as Gisella to scroll through slowly is just listing the number of reports that the SSAC has produced in the last three years. As you can see, they fall into a number of categories. The first category is DNS security in general and there were quite a few reports – about seven reports – produced in that category. One report on DNS abuse, one on internationalized domain names, two on WHOIS data, and then finally the SSAC produced three reports to assist the community to focus on relevant aspects of the IANA stewardship transition, primarily, if you like, supporting, not to express a view, but to support the rest of the community in understanding what the IANA functions were about, what the contact covered and the sorts of things that ought to be considered in a transition proposal.

Finally, again very recently, the SSAC has provided a short comment on the proposal of the CROPP Community Working Group on ICANN accountability enhancement.

It has been, for a small group of between 30 and 40 people, it has been quite active within the last few years considering the amount of reports raised.

I would now like to hand over to Dave Piscitello and Richard Lamb to expand a little bit more on ICANN staff role and activities. Thanks, Dave.

RICHARD LAMB: Dave, do you want me to go?

DAVE PISCITELLO: Oh, thank you very much. I'm here. Thank you very much for inviting Rick and me to speak today. I'd like to [inaudible] of formal talk that Rick and I give and give you all opportunities to ask some questions about what our day job looks like because it's probably very different from most of the ICANN staff. We have some very different interests.

What I'd like to do before I use my slide is talk a little bit about one of the points that Julie raised, which was the definition of security, stability, and resiliency. In particular, I think that the part of the SSR that gives us a little bit of room to navigate in the very tricky space of trying to deal with abuse in particular is Julie explained that stability has to do with the system operating as expected.

For the most part, I think that the ICANN community tends to think of that in terms of [inaudible] spirit. I tend to be a little bit more spirited, as many of you know.

One of the things that I always argue with people who say, “Well, this is not in your remit and that is not in your remit,” is the system is expected to not return [inaudible] harmful answers. It’s not expected to vet criminal activity and terrorism and bullying and all the child trepidations that Internet users face.

In my mind, and it’s very loosely interpreted, the system is not stable if it’s not giving honest answers. It’s not stable if it’s creating opportunities for abuse or it’s creating the potential for [inaudible] or financial harm.

This is going to become even more pressing as we evolve to [inaudible] it is today. Our team doesn’t judge content and we don’t direct action or take direct actions on the [retention] of domain names. We don’t take direct action involving our contractual agreements with ICANN’s contractual partners.

We do collaborate with them. We collaborate with law enforcement. We collaborate with other security researchers an academia. We facilitate conversations to try to bring communities together so that legitimate court instruments can be executed in a timely fashion and actions can be taken to dismantle global botnets that are creating chaos in the Internet.

GISELLA GRUBER: Dave?

DAVE PISCITELLO: Yeah?

GISELLA GRUBER: I'm terribly sorry to interrupt you, but the interpreters are struggling to hear you. So if you're on a headset or a landline or a cell phone?

DAVE PISCITELLO: Well, I am on a mobile phone, but that's really the constrain of where I'm calling in from.

GISELLA GRUBER: If you could maybe speak closer to the phone, closer to microphone. We're just trying – both French and Spanish interpreters are struggling to understand.

DAVE PISCITELLO: Okay, is this better?

GISELLA GRUBER: I'm just getting confirmation from the interpreters. I do apologize for the inconvenience.

DAVE PISCITELLO: Well, let me continue, an if it's not working, let's just try to – I'll try to go off speakerphone and see if holding the handset works.

GISELLA GRUBER: Please. Thank you.

DAVE PISCITELLO: Having a little bit of a context for some of the activities that we engage in, I'm trying to find the slides here. I've got to go one more, and maybe one more, and maybe one more. Is there another slide deck? I'm only seeing the slides from Julie here. Hello?

UNIDENTIFIED MALE: I hear you, Dave.

DAVE PISCITELLO: Oh, we're just switching decks here. Oh, thank you so much. One of the things that our team does that is a little bit of a departure from the way that the rest of the world views SSR is we have to consider not only domain names, but all the identifier systems that ICANN is responsible for overseeing.

That includes coordination with the regional Internet registries on the Internet address allocation abuse, autonomous system number abuse. It includes consideration of any of the registries that ICANN either manages directly or provides some oversight for.

By advancing a slide, I'm seeing [inaudible] functional areas and nothing else, so I'm going to see if I can at least get to my slides so that we can proceed. Oh, perfect. We're competing here.

Okay. We look at our roles as defined four functional areas. Perhaps the one that people are least familiar with, but one that is almost a 24/7 activity for many of us in the SSR team is what we call threat awareness and preparedness.

It's closely associated with what we call trust-based collaboration because one of the things that our team does is spend most of our time in an external-facing capacity. We are very often the only recognized bridge between contract parties like registrars and registries and law enforcement and security community.

In situations where there's a threat to the identifier system, John Crain in particular is literally the SSR rolodex. He has the ability to reach out to nearly every ccTLD, as I believe Rick probably does, and finds someone there who is technically competent to help address an issue or to help mitigate threats.

The kinds of activities that we often get called in to assist with are liaising between ICANN's registry or registry liaison, between the registry and registrar's proper and legal counsel in situations where law enforcement in a multi-jurisdictional capacity will seek a court order to dismantle a botnet.

I think some of you may be familiar with Ransomeware, and Randsomware is a kind of infection on your computer, and what the

Ransomware [inaudible] have done is created a fairly malicious package that will encrypt all the data on your computer and then hold you ransom. If you don't pay a fine or a fee within 24 hours, they will throw away the key and you will lose your data forever.

This is a particularly nasty scam, and for a number of months, law enforcement were chasing a Ransomware criminal conspiracy that was known as Gameover Zeus and Cryptolocker. In [inaudible] Cryptolocker activity, John and I were asked to assist in arranging correspondence and communication between the registries where the domains were being registered in order to sustain or maintain the botnet. We helped with the technical details that would eventually make their way into a court order that explained what the law enforcement agents would want to see executed once the court orders were issued.

Over the course of many, many months, we were [partied] to trying to make certain that on a given day at a given time in multiple jurisdictions, court orders would be executed, the registries would do what they needed, law enforcement would cease equipment and apprehend conspirators. It was a very successful [inaudible].

That was a very interesting process for us. It was also I think beneficial to the community. It restores, in my mind, stability to the Internet. We didn't have to worry about getting online and being held for ransom.

Part of the reason that works is because John and I and Rick and Carlos and Steve are all known in security communities. Many of us work very closely in either mailing lists or other collaborative environments and

share information about investigations. These are not always [inaudible] investigations. Sometimes they're spam. Sometimes they're trying to identify people who are running illegal pharmaceutical affiliate programs or who are running counterfeit goods scams. Even these 419 or Nigerian scams, things like stranded traveler and others, are the kinds of activities that we monitor.

Having been in security for 25 years, these are things I did before I came to ICANN and things that John did when he was at CENTR. We are involved, we're trusted, and we're able to bring people together to try and help come up with ways to solve problems, ways to mitigate threats.

One of the things that we're now trying to do falls under this title SSR analytics and this is where one of Rick's talents – he's an excellent programmer – is coming to the fore. We're trying to look at the new TLD program for I think the first time in ICANN's history gather our own information and understand from our own research and our own analysis of all the data that ICANN can collect from. For example, the L-root system or from our partners who provide phishing [inaudible] like the APWG, the Anti-Phishing Working Group.

Rick is actually working on a program right now that's going to help us track phishing in the new TLD program. Is it more than the legacy TLDs? Is it less? If so, more or less, why? We're going to start asking questions like that.

Within that analytics project, we were also doing things like investigating the characteristics of verticals in the community, financials, or others and try and understand how they use WHOIS. Are they leaving themselves exposed to some sort of criminal attack because they are not providing adequate measures to make certain that their domains are not hijacked. Those are all things that we do that I think most people aren't that familiar with.

The last I think is one that a lot of people are familiar with because we touch so many countries, and this is again one of the places where Rick excels and spends a lot of time and I'll let him talk more about it.

We spend an awful lot of time and do an awful lot of travel delivering training. Our capability building programs allow us to go to countries where they do not have access to subject-matter experts like Rick or like some of the people that we contract through the NSRC. We are able to go to countries and explain how to build networks, to build secure networks, to create secure registry operations.

About three years ago, almost four now, Bobby Flaim, who is a supervisory special agent with the FBI came to me and said at an ICANN meeting, "Could you explain to us how the DNS works? How are people actually doing some of these investigations?" From a 30-minute conversation at one ICANN meeting I was asked next time to do an hour, then two, then four, and at this point we've grown that program of providing law enforcement with knowledge so that they can conduct investigations into DNS abuse and misuse to something that can easily run a day-and-a-half, perhaps two days. We're now doing that in all five

regions. Carlos Alvarez is delivering it in Spanish in Latin America. John and I and Steve Conti are doing it in Europe and Middle East. I've been doing a lot of it in North America. Champika Wijayatunga is a part-time global stakeholder engagement staff and part-time security staff spends I think all most all his life on planes or doing training. At least that's what it looks like on the basis of a number of times he's delivering this kind of training.

It's been very, very well-received. We actually received a nomination for a World Summit on Information Society project prize. We didn't win, but just to be nominated was quite exciting.

We have a lot of different activities, and I think I'm going to stop there and let Rick talk about some of the things that he's been doing so that we have maybe another 20 or 30 minutes at the end of the time for you guys to ask questions to us about some of the other things that you might be curious. Thank you.

RICK LAMB: I'll pause for a minute to see if there are any questions before I start. Hearing none, that capability building that Dave brought up I wanted to make clear. First of all, thank you for entertaining and listening to us speak. I know sometimes we get too excited and we move a bit quick for the interpreters. I'll try not to do that.

The capability aspect, I think if Dave didn't emphasize it enough, is the trust that we build in those exercises. Whether it's law enforcement or DNS or building a secure network, I always look at that as being it's not

the textbook knowledge, it's not even the hands-on knowledge that we're giving. All of this is very valuable. But what's most important is the week or the few days that we spend immersed with each region and the people in that region that are interested in a topic and the networks there then created between those people. The human trust networks, as I always look it, are more important than the computer networks because if something does go wrong and there is some sort of a threat, it's that human network you're going to have to engage.

It's not like we're going around just providing information one way and getting, say, law enforcement some sort of help in finding things. It's more of a two-way street so that the communication links happen.

Now I'm going to back up for a second. One of the nice, interesting things about our SSR team is we are very different people. Dave and I fight all the time. Very different views, which is a good thing. I wake up every morning actually doing a sanity check. Why am I still here at ICANN? What am I doing? We're all in this business and on this call probably because some part of us cares about what the final result is.

One of the questions I like to ask while I'm doing that sanity check is, "What if we weren't here? What if ICANN was not here? What if the Security, Stability, Resiliency Team was not here?" There are aspects of that that have confused me for a bit. I used to work in the US State Department and was involved in the turning in the WSIS into the IGF and adding one of those S's in the SSR. I sometimes wonder what good does this all do and what would happen if we weren't here?

The natural answers I come up with that is, of course, if there's no one coordinating the root zone or the IP addresses or the protocol numbers, there would be duplicates and things would not work.

As Julie said earlier very eloquently, there's certain stability for businesses that we provide. Businesses hate instability. Stability is critical to innovation, to the economic wellbeing of many, many efforts.

You often hear about alternate routes, and every time you say that there's always a part of the room that gets all scared and jumpy and stuff like this because this is the worst thing in the world. It's not so bad in and of itself other than it sometimes distracts people from what's important.

As I'm doing this sanity check, I say, "Well, what controls do we have?" Again, I have to hand it to Julie for being so clear in describing some of this stuff. We have no statutory authority on the root. It's just a file. Anybody can go to anybody. The only reason they use our root zone file is because we're good at making people like us, and that's something that I think is often lost. There is no – we have no power, which is interesting.

So I continue to ask the question: why am I here? This sounds like a precarious organization. But there are a few things we can do. Not only some of the training stuff, which I'll get into in a minute, but we do have these agreements between the various registrars – for example, I'm just going to pick one – that allow them to sell. I'm sorry I'm going to be very direct here because this is how I justify it to myself. Those agreements

allow some registers to sell dot-com domains. That's a money maker. Just follow the money.

That's a lever that we therefore then have over, let's say, registrars, for one example. The Compliance Team deals with that. Then the question comes to my mind: are we policemen or are we partners? Well, again, as Dave pointed out as well as Julie pointed out, we're partners. We're partners with the community. I think this is where our largest contribution is. Not only the training, but acting as a coordination point for some of this threat awareness and preparedness.

Our key functions that the SSR team provides, a lot of it goes unnoticed because a lot of times these things happen quietly, as they should. I think that's something that's hard to point out. There's very little, if any, other coordination points like ICANN.

Then the training that we do is again something that does build this fundamental trust between people. I love quoting this guy from the Department of Justice. He says, "You know, at 10:00 on a Saturday night, if I get a phone call from something related to my work to take down some website or something like that," if it is through some hierarchy through his company through he different channels of command, he's on his time off. He's not going to answer the phone.

However, if he's spent time with his counterpart, say, in Estonia, having beers relaxing with them in a law enforcement training class held by Dave and John, he will most likely pick up that phone and deal with the problem, solve it and it'll be done with right away. His point was

specifically against [ITU] efforts like impact versus bottom-up efforts like what we do. A lot of his training things, that does solve the problem in a much more effective way.

We've done an awful lot of things here as far as coordination, and of course we don't just limit our work to the DNS as maybe we should, but oftentimes we are called upon to be experts in other areas. For example, the OAS has called us a few times on creating national cyber frameworks for various countries and [very impressive] work by our friend, Belisaro, from OAS.

But we get called in because of our experience in the multi-stakeholder model and because of our ability to encourage a light regulatory approach, yet still encourage a rule of law. Of course our relationship with the ccTLDs is key.

That's what I do every day to convince myself that, yes, we are still doing something very useful. Of course there is – I hesitate to bring up DNSSEC because that is something that's near and dear to my heart and it's something that I was key in making happen as far as getting the root signed. That's a different aspect of what we do in the SSR team and is critical in many ways, not just to secure the DNS which is how it's often simply portrayed, but the real reason all us geeks get up every morning and care about this thing is DNSSEC deployed to a certain level ends up creating this global secure database and nothing like that exists.

If we could get enough people to deploy this, a certain critical mass, then all of a sudden Internet of Things, the various – the smallest item

at the edges of the Internet, every single device will have at least something that they can hang their hat on for security, something to get a secured delivery of either key material, not just a domain name or an IP address, but something else. That is an entrepreneur's dream. This is an opportunity for everything.

I admittedly often end my talks and trainings with a spiel on how to apply for patents and start a business, because this is something I've done in the past many, many times and every time I see – sorry, I get kind of excited here. Every time I see a classroom full of people, younger people particularly, that seem to be afraid to take a chance, I just lay right into them. We have long talks about things. A lot of times, it's nothing they can do, rule of law in their country, etc. Instability within their current government, etc. But I try to show them that there's a lot more that can be done here, and at the DNS and ICANN in particular with its very generous and broad programs to try to help societies not just about DNS and IP addresses and so forth.

With that, I've been here for over seven years, so I guess the sanity check keeps working. That's it for my end. I don't know if Dave . . . ?

DAVE PISCITELLO: I'd love to spend some time just answering questions about whatever SSR issues you'd like to learn about. If you want to know some of the [inaudible] of any of the functional areas that we talked about, I'm happy to give some more examples.

RUSS MUNDY: Thank you very much. Do we have any questions? We have well over a half an hour. Holly?

HOLLY RAICHE: Yes. First a comment and then a question. One of the things I do is teach communications law, and for the lawyers in the room, you would know that jurisdiction is an issue and jurisdictions kind of end in borders [inaudible] ocean.

Increasingly, I use the ICANN diagram to say now that we in fact in a global communications, that the [inaudible] of problems are offshore. What do you do about the problems offshore? I found this really interesting because it's the missing piece that says when things go wrong, this is where you go and this is where your law enforcement agencies and your security people and so forth go, even though it's not, if you will, doesn't solve the jurisdictional problem; it solves the actual practical problem.

So thank you for that because maybe I can just say keep getting up, Rick, because you're needed in the scheme of things and in what I teach.

I think my question was – and maybe Dave knows. I've read a lot to of all the SSAC documents. What I know, they're only voluntary, but how useful do you find them and how useful is it to say what do you do to make sure that people listen and read them and then take notice of them? Thanks.

DAVE PISCITELLO: I think you're asking how useful are [inaudible]. Is that correct?

HOLLY RAICHE: Yes, very.

DAVE PISCITELLO: I have a couple of different answers. I spend so much more time outside the ICANN community than inside the ICANN community. One of the things that I'm always startled by when I come back to the ICANN community is how tiny and incestuous the community is. And I don't mean that in a malicious way. I just mean that the ICANN community tends to believe that it's like the biggest thing in the whole world and that the world revolves around the DNS and if the DNS went away or ICANN went away, the DNS would stop.

I have to laugh because we're a tiny fraction of what goes on. As Rick said, ultimately, with respect to the operational parts of the DNS, it's a generated text file. I know it over-trivializes it, but it also puts it into context.

The operational [surface] that ICANN actually influences is microscopic by comparison to the number of end systems and the number of systems that resolve domain names to Internet addresses all over the world and the different organizations that don't have contracts with ICANN that do this. That's where I spend most of my 22 waking hours sometimes.

One thing I would say that SSAC documents have had a very, very good impact inside the ICANN community. Having said that, it's like saying that a tax report has had good impact on the one percent in the US economic structure.

I would love to be able to figure out ways – and I'd be happy to sit down with Julie and others in [inaudible] to say how do we actually amplify this signal and get other people to understand some of the things that SSAC has said? I think especially some of the more recent reports that SSAC has put together on search lists and on credential management. They're great, but they're not going to reach a lot of the people that actually need them.

I find frankly that I reach more people summarizing an SSAC document on a blog post than all the hits on some of the documents that we've published over five years. That's probably not a good indicator.

One of the things I would like to be able to do is figure out how do we actually get this message to other people? We do only reach a small fraction of the people who actually need to hear these messages.

RICK LAMB: Dave, I agree with you. One of the things I'm sure you've hear, too, and I've heard a lot from non-community members, people from outside the ICANN community, is that we do not include a lot of the operators and the people who actually have to deal with these things on a day-to-day basis.

I'm not really sure how to bring them in. Most of them, when they see the word policy, they tend to run the other way. But there is definitely kind of a missing element to the operator community who would feel the pain. I've just going to get down to basic stuff here. They need to feel the pain to want to read the SSAC documents.

DAVE PISCITELLO: Rick, you touch on a – I don't want to make this a conversation between you and me.

RICK LAMB: It always is.

DAVE PISCITELLO: You touch on a point that has always confused me about the organization called the Generic Names Supporting Organization. One of the constituencies to me is remarkably absent are people who run large enterprise networks or large ISPs. We have constituencies, but when I go and I see who participates, I don't see an [Akamai]. [Akamai] delivers more content than anyone. I don't see PayPal. I see PayPal in the policy part, but I don't see them asking – this is something we need to pay attention to.

Some of the ways that our contracts with registrars or contracts with registries are written, clearly they're multi-stakeholder but not all the stakeholders. I'd love to be able to figure out – and maybe crossing the beams here, but I'd love to be able to figure out how you actually get

some of the stakeholders that have a stake but aren't present in policy making.

ALAN GREENBERG: Thank you very much. I don't know what's happening with Adobe Connect. Mine disappeared, it came back, and I now see a message in the chat area attributed to me that I didn't type in. I don't know if Adobe Connect is working or not. If anyone wants to speak, and I don't see a hand, just yell please. Somebody saw my man in the middle attack is working.

CHERYL LANGDON-ORR: Now is not a good time to confess to that, come on.

ALAN GREENBERG: Someone typed in "Look at how fast people are dropping off" and has my name on it and I didn't type that. As a matter of fact, I wasn't connected to Adobe Connect when it was typed.

CHERYL LANGDON-ORR: Oh, now, that's worth bringing up with someone in security.

UNIDENTIFIED MALE: We don't have any critics at ICANN, do we?

CHERYL LANGDON-ORR: They could be involved.

ALAN GREENBERG: This is quite fascinating. In any case, we have a smiley face, but no hands. So the smiley faces are working. There are no microphones, so no one is any longer connected via Adobe Connect and speaking on it. Now all the microphones just came back.

CHERYL LANGDON-ORR: Staff has control of that, don't they?

ALAN GREENBERG: I don't know.

CHERYL LANGDON-ORR: Man in the middle. All I've got on the screen are questions.

ALAN GREENBERG: Anybody want to say anything? I'm going to type a message to see whose name comes up?

HEIDI RAICHE: I've got multiple [inaudible] typing.

ALAN GREENBERG: All right.

UNIDENTIFIED FEMALE: [inaudible] who is this?

ALAN GREENBERG: All right. Other than fascination with Adobe Connect, are there any other questions for our guests? Olivier to the rescue!

OLIVIER CRÉPIN-LEBLOND: Thanks very much, Alan. I have a question with regards to DNSSEC. Following up on a discussion I had last week at one of these conferences, someone came to me said, "Well, this whole thing of DNSSEC is a bit of a problem as far as security is concerned because when you are going to have a signed domain, the whole structure of signed domains from the point of your domain all the way up to your provider and the top-level domain, etc., all of that needs to be signed. And if there is somewhere along the way some kind of a problem, then your domain is not as secure as it should be when DNSSEC is used."

I was a little confused on that and I wonder whether someone can reassure me of this, what appears to be some kind of a weakness in the use of DNSSEC.

RICK LAMB: I can probably even guess who that person is. It shows you how small this community is. First of all, he is not wrong. DNSSEC requires that the

root and the ccTLD be secure. That's two steps along the chain. Then including yourself, if you're Google, you have to trust yourself.

If you assume that the root and Google are fine, then it's the ccTLD that you need to be concerned about. So he is correct, but I would argue that you are still net positive because you have now some sort of mechanism to check the validity of the response that you're getting from the DNS.

Now, even if that relies on these three other parties, the root, the TLD and yourself, that's still better than where you were before. Just to cut to the chase, oftentimes I am asked, "Who should I registrar my name under?" Again, putting my business guy's hat on, well, who's got the deepest pocket to sue?

Then I go after, I say, "Just register with dot-com," or, "Dear friends at Verisign." I hate to say that, but they are a large organization who has by judging their press releases and stuff has tied their wagon at DNSSEC.

The short answer is he's right, but you're still ahead of the game because now you have a response that has been cryptographically verified, and instead of anywhere along the line someone being able to lie to you – for example, your connection between you and the ISP, that wire going across the telephone poles or the co-ax, or whatever, fiber if you're lucky, can be intercepted, modified, and changed. Could change a response to the DNS question you posed. With DNSSEC, you're limited only to the one intermediate stop.

There are two different groups of people out there, the certificate authorities out there who sell you the digital certificates to secure websites see DNSSEC as competition and they have regularly been throwing up excuses and sand into the gears to not deploy it. His excuse is a lame one. There are much better ones out there, such as [Akamai] not supporting parts of DNSSEC, but other than that . . .

Does that answer your question?

OLIVIER CRÉPIN-LEBLOND: Yeah, that's great. Thank you. I do have a follow-up also DNSSEC related.

RICK LAMB: Sure.

ALAN GREENBERG: There's no one else in line, so go ahead.

OLIVIER CRÉPIN-LEBLOND: Okay. Thanks very much, Alan. My other question is also relating to DNSSEC and that's with regards to the recent political developments in Washington, DC, with questions around encryption, around encryption keys. In some European countries, there are also some questions regarding the use of encryption and encryption keys and strong encryption, whether those keys should be given to the law enforcement

agencies, whether there should be – well, whether they should be allowed to have strong encryption keys.

RICK LAMB: Wow.

OLIVIER CRÉPIN-LEBLOND: So the question then is how does this affect the viability of DNSSEC worldwide?

RICK LAMB: Wow. That's a really good question and I'm sure Dave is going to jump into that as well. Certainly we don't control politics. As far as the root's concerned, I can speak authoritatively. I'm the guy who designed most of that and wrote software. I know where the hardware comes from. Sure, it comes from a town outside of London, so GCHQ and NSA, well, whatever that arrangement is.

But as far as any – we've never had any suggestions, visits, or anything from anyone in the US government, any government, as far as wanting access to this thing. In fact, just to be safe, I even contacted some of my old pals in NSA before this thing happened and said, look, it would really be awful in the eleventh hour you came up and annoyed us. You're not going to, are you?

Anyway, they said, “Absolutely not. You guys are doing great. This is fine.” Take that for what it’s worth. Maybe that’s good. Maybe that’s bad.

My point is I have no control over the higher-level politics, but at our level, we’ve been very transparent about it and I’m proud of that because we do have these 21 people from around the world, and we’re about to select new ones, that actually hold bits and pieces of credentials that are needed for us to even access that piece of hardware. You couldn’t even get at the hardware without an international [inaudible] of people to do this. That was all my intention to make it so that even if you didn’t trust ICANN, you trust these people.

I don’t know. Dave? Political, outside of this, it’s very hard for me to say anything because I just don’t know. I certainly hope it doesn’t go the way that some of the bills are headed in Washington.

DAVE PISCITELLO: Well, it’s not just Washington. If you looked at what some of the comments and statements that have come out of the United Kingdom and some of the proposals, worldwide about encryption right now, I don’t think ever in the history of mankind have so few people been so massively uninformed in a position to create such irreparable harm as the people who are trying to promote agenda where we create backdoors of encryption or we prohibit encryption or we prohibit the export of what’s called intrusion software. I don’t know if any of you have followed this [inaudible] Act.

It's just absolutely comical if it weren't so scary. I spend a lot of time with people on mailing lists who are much, much more well-versed in encrypt analysis and cryptography than I am and they are mortified.

GISELLA GRUBER: Dave?

DAVE PISCITELLO: Yes.

GISELLA GRUBER: Sorry to interrupt. There's no interpretation currently. We can't hear you.

DAVE PISCITELLO: Well, I have it about as close to me as possible, so I'm uncertain what we can do at this point. It might also be that I talk too fast when I get passionate.

I think that especially because there are so many civil society implications about what's going on, encryption [inaudible], that there's probably a very meaningful role for ALAC to look at what is being suggested in many of these bits of legislation.

The real threat and the real insanity of it all – I mentioned earlier today I was talking with members of the Anti-Phishing Working Group and we were discussing legislation. There is a bill under proposal that would

prohibit the export without license of what is categorized [inaudible] intrusion software.

If you actually go and look at the definition of intrusion software, I would argue that it is anything that you would legitimately use to test networks to see if they're secure. In fact, you could probably claim that the little bit of software that's in every laptop and mobile device that resolves domain names to be considered intrusion software.

Where I think most people who are not familiar with cryptography and internetworking and security are going off the rails is that they seem to confuse what a piece of technology does with the intent to use that technology. They think that those two things are tightly connected.

The problem is that almost all the tools that [inaudible] uses are tools that we originally used for networking diagnostics. They've been taken to the next level or they've been modified. The criminals have to use exactly the same protocols and exactly the same domain name system as we do. And they have to use the same cryptographic mechanisms if they're going to be able to use commercial off-the-shelf software or open source.

Prohibiting people from doing the real practical day activities, the things that make the Internet meaningful and enriching and commercially useful can't be really separated from the things that are exploited to abet criminal conspirators or terrorists or state activists who are intent on exfiltrating information.

I find it really unnerving and I think that a lot of people who are in the ICANN community and in At-Large could lend their competency to this argument and say, no, you're actually going to create serious problems. You're going to inhibit the ability for people to express themselves freely, to engage in lawful, rightful activities. I'd love to see more activity from [inaudible].

ALAN GREENBERG: Thank you very much. There was a question in the chat about "Is there anything people in At-Large in the communities around the world can do to increase the implementation rate of DNSSEC? Any thoughts?"

RICK LAMB: Wonderful question. I appreciate that. I think it's simply raising awareness that it provides security, specifically having websites signed or the domain names that websites use to have DNSSEC deployed on them. I think it's critical at this point.

These can be used as [inaudible] motivations could be that it's a differentiator that allows you to provide something that this is slightly more secure.

Right now, we are at 80% - over 80% - of the TLDs are signed. Most anyone could probably deploy DNSSEC. The resolvers, the side that validates this thing that the ISPs have, that's about 25% at this point and growing. That's amazing how quickly that's growing.

The only piece of the puzzle that we're missing is the website gets signed. That should not be a hard thing, but we do need people to, first, know what it is and if they need training, certainly ask. We offer free training, hands-on training. Start a dialogue if through you guys or someone else, just to find out what the barriers are.

The current barriers I have found with, say, the Fortune 500 companies or the top, let's say, online properties through Alexa 500 I think it's a list, is that they sit behind something called content distribution networks. They sit behind these massive systems that share the load for websites so that they can respond quickly.

These systems break DNSSEC. Specifically, they break [Akamai's] content distribution network. It literally does come down to a very small set of people that are making this difficult.

The way ALAC could help is if you encourage the customer to ask for it, [Akamai] will roll, will take care of it. CloudFlare I think is an organization that's competing with [Akamai], although much smaller than [Akamai]. They're going to deploy DNSSEC across their platform. Just have it free, just built in, to their platform I think in a month or two. That will be another motivation for [Akamai] to catch up.

Thank you for the question. That's very helpful.

ALAN GREENBERG: Thank you very much. I would have thought that if a few of [Akamai's] largest customer say, "We demand it," it would happen. It really comes

down to those customers who are critical, large users of [Akamai] to actually care enough about it.

RICK LAMB: I guess that's not enough. The US government—

ALAN GREENBERG: And I don't think we have any influence over them.

RICK LAMB: No, we don't, and many of them have asked. US government, the military, has asked and they have not provided a reasonable way to support it because it fundamentally changes their design.

ALAN GREENBERG: Understood. Any other questions? We still have another 15 minutes if anyone wants to do it or we can give people back 15 minutes of their lives.

CHERYL LANGDON-ORR: I'm not sure I can afford that much spare time. It's not like I'm leaving my country tomorrow or anything.

ALAN GREENBERG: Try sleeping, Cheryl. Some of us use that to buy a bit of time.

CHERYL LANGDON-ORR: Can I just say, like sex, that is way overrated. And yes, I know that is going to be translated and transcribed. Feel free to quote me.

ALAN GREENBERG: I won't ask you to go into details, then.

CHERYL LANGDON-ORR: Well, not on this call, Alan.

ALAN GREENBERG: Olivier, is that a new hand or is that an old one?

OLIVIER CRÉPIN-LEBLOND: That's a new hand, Alan.

ALAN GREENBERG: Then I guess you have the floor.

OLIVIER CRÉPIN-LEBLOND: Thanks very much. I have another question with regards to DNSSEC. This is to do with the cost of rollout in DNSSEC. As you know, a significant number of our At-Large Structures are based in countries which are development economies. I just wondered whether there was any additional infrastructure and likely high costs for rolling out DNSSEC in

those countries, when you compare it of course with having a DNS that is unsigned.

RICK LAMB: Well, yes, there is additional work. If I'm understanding the question right, there's additional work and most of the time the problem in some of the developing organizations or countries, the organizations in some of the developing countries, is not intelligence staff – they have plenty of intelligence. They have intelligent staff that are very, very capable. I can attest that because many of them have been in my class and I've just been blown away. But they don't have enough.

Typically, it's one person maybe having to deal with all of IT and the last thing that he needs or wants, and I would even recommend against, is to deploy DNSSEC in some sort of a haphazard fashion.

In that respect, yes, it's additional cost and it might be prohibited. The flip side of that is organizations like CloudFlare and others are starting to offer as part of their hosting service, and I know many of the websites from various parts of the world are, for better or for worst, hosted in Miami or somewhere in the US.

So if you go to a hosting service that will take care of all this for you, then the cost is the same as it would be someone here that would be taking the same route.

I think in the long run, that's the direction this stuff will take. Talking to the large companies, most of them, unless the web is their only

business, outsource the hosting of their website and often even the management of their website.

So the focus should not necessarily be on – the problem is not necessarily the company itself, but it's the people offering the hosting service. Of course if you get the end users to ask for it, then they'll maybe find a hosting service that offers this.

I wouldn't say specifically cost is a problem. It's usually resources, cost may be the same thing. It's not enough personnel. At the ccTLD level, for example, that is often the case. You have very sharp individuals that are some of these places, but there's only one of them. That puts a burden on it.

I've changed my tune lately. Maybe my boss will try to fire me for this, but if they're not ready, don't deploy it because I'd rather see someone deploy DNSSEC – a good installation of DNSSEC that'll work than just tossing something together quickly and then having it fail later and give the naysayers, like those which you've spoken to, fodder.

ALAN GREENBERG: Thank you very much.

DAVE PISCITELLO: There's a question in the chat that was directed to me about taking the DNS abuse crusade through all continents, including Africa and the Middle East. I'm sorry, I can't pronounce the name – Nkem Nweke. Is that right?

ALAN GREENBERG: Go ahead anyway.

DAVE PISCITELLO: He was asking where have we gone so far. I just returned from Cairo where I did a training and I've done a training in a Lebanon and will be returning there. I know we do quite a bit of ccTLD training in Africa and Rick probably can list some of the places where he's been. Often what we do is try to run some of our training in conjunction with regional AfriNIC or Africa Cert organizations.

The other question that was asked is how do we actually arrange engagements? The engagements normally come to us either through requests directly to our staff or through requests that are submitted to global stakeholder engagements. There's no real formal path. We don't have a sign-up sheet, so to speak. That's partly because we don't have the staff capacity yet to deliver this as much as we would ideally have. Part of that is a chicken and egg. We're so busy trying to deliver the training that we haven't been able to actually put together the kinds of material that would allow us to effectively train trainers. We're trying very hard to correct that, but in the meantime, it's very hard to say no.

We're stuck between a rock and a hard place. Two years ago, I was the only one who was delivering this. Now everyone is delivering it but Rick and Rick is learning it.

One of our problems is that it's a very unique course and it requires a fair amount of hands-on and involvement in actual investigations to deliver effectively. It's going to be a slow path to actually be able to put together train the trainer programs and something formal enough where we can ask in the same way that people ask today for the ccTLD focused training.

ALAN GREENBERG: Thank you very much. Anyone else? I saw Alberto's hand up a while ago, but it's now gone down, so I'm not sure if the question was answered anyway. Anyone else with any questions? We have a few more minutes left.

ALBERTO SOTO: Alberto Soto, if I may take the floor.

ALAN GREENBERG: Yes. Please, go ahead.

ALBERTO SOTO: This is my question. Technically, DNSSEC is deployed or rolled over in several systems. Is that correct? Because you mentioned that maybe if provider rolling over DNSSEC, then the cost is not going to be the same as another provider. On what system is DNSSEC implemented or rolled over and is it similar to other security systems already in place? Thank you.

RICK LAMB: DNSSEC is really who, not what, that it's been rolled out on. There are very few right now hosting providers that provide DNSSEC support. GoDaddy does. CloudFlare does. And there's a whole bunch of them in Northern Europe I know that also provide this.

But we're talking about less than a percent of the hosting providers right now support DNSSEC. That's the problem. Once you start having more and more of them starting to support this, then your average company or organization can simply do what they do now. When they go to order their hosting service for their website, they click an extra box and it's just turned on. That's what we would like to see.

DNSSEC by itself, sure, the geeks can implement this. It's not actually that hard, but it's not what I would expect your average proprietor to do themselves.

The focus – and this is back to the point that we need to get more the operational community at ICANN meetings. It's the operational community that has to hear this message that need to figure out ways to deploy it, and they'll come back and say, well, this is difficult, this is hard to do, this is a technical problem. Good! We need that dialogue to happen because that's the only way those problems will get solved.

Right now, if I talk to somebody in a large organization, they'll say, "Well, I read this about DNSSEC and it looked like it was kind of hard to implement, so I just went and did something else." Mostly they could

say that because there's no end user demand. If the end user started asking for it, of course they would treat it differently.

So, to answer your question, essentially none. No one is supporting this other than CloudFlare, GoDaddy, of course a bunch of boutique small hosting providers support this, but it's not in mass where anyone can do this.

It is an opportunity, though. I'm putting my entrepreneur hat on. It's an opportunity for somebody, a small hosting provider somewhere, any place in the world to say, "Look, we will provide fully managed hosting and also provide DNSSEC for your website." This has been – differentiating using DNSSEC has been an example for companies. There's a large ISP in the US called Comcast. Over 20 million people. They support DNSSEC. That was their reason: differentiation. People care about security now. This is not all, but it's another piece that they can add to their security marketing portfolio.

Sorry. I wish I could answer that better.

ALAN GREENBERG: Let me ask a follow-on question. You said the operational community, the web host, hosters, and other people who we need to convince don't come to ICANN meetings. What meetings do they go to and why don't we go to them?

RICK LAMB: I try to go to them. Dave, if you think of some ones, please chime in. I met a lot of them at a [MAWG] meeting recently. Dave's bailiwick – hello? I'm getting music now on the line.

ALAN GREENBERG: I think they're telling us there's three minutes—

CHERYL LANGDON-ORR: That's a musical interlude. It's fine.

RICK LAMB: Okay. All right. That's so romantic. I think there's [MAWG] meetings. They're [NANAOG] meetings, which are things that ICANN does participate in often. But there are also – we need to get at the guys that are not simply trying to connect the networks together. We need actually to get to some of the hosting providers as well.

I'm not sure. I would like to find them. I've presented at RSA meetings. I presented at [Interop] meetings. I think those are our critical pieces. Working more closely with the vendor community. Without getting too soiled, but working close with the vendor community I think are good ways to get the word out. When I talk to people in the vendor community, I often get, "DNSSEC what?" And I'm like, "Wow, how could you not know this? This is right up your alley. You're selling servers and hosting equipment."

I guess that's a homework item for me to try to get a better handle on how to contact the operational community, if there are any regular events they go to and maybe how to get their attention. I think ISP CON might be one. I'm just thinking of the few ones that I've seen pop up and I've gone to and given my awareness training spiel.

UNIDENTIFIED MALE: Rick, there's always Paul Vixie's standard response of "How do you get anybody to implement something that they're either reluctant to implement or can't justify financially?" You included as a requirement for US government purchases, then everybody implements it because they have to.

RICK LAMB: Well, it is a requirement for US government stuff already. They have implemented it. Poorly, but they have implemented it and it's still – that hasn't born fruit other than within the US government.

UNIDENTIFIED MALE: That's odd.

ALAN GREENBERG: End on time because of the interpretation. I thank you all. As one suggestion, however, if you want to find out where do the web hosting companies and such go, look to the people who provide rack-mounted engines they run and find out where they sell them.

RICK LAMB: That's a good idea. Okay.

ALAN GREENBERG: They must sell them at conferences somewhere. Tradeshows somewhere.

RICK LAMB: They do. All right.

ALAN GREENBERG: I thank everyone who presented. I thank all the people who came to participate in this teleconference, this webinar. Great attendance. I think we've all learned something, and I wish you all well for the rest of the day.

PARTICIPANTS: Thank you for having us.

CHERYL LANGDON-ORR: It's been excellent.

GISELLA GRUBER: Thank you very much. The webinar has been adjourned and the audio will now be disconnected. Thank you very much for joining today's webinar.

[END OF TRANSCRIPTION]