SAN JUAN – ALAC & Regional Leaders: Work Session, Part 11
Tuesday, March 13, 2018 – 15:15 to 16:45 AST
ICANN61 | San Juan, Puerto Rico

HOLLY RAICHE: …going on. Today, every single bit of mitigating [inaudible] we can to minimize the danger. It would have the advantage of ICANN being on the front foot, being seen to support users as much as possible, and being seen to provide as much information and assistance as possible. Really, those are the only conditions I'd be happy to move forward.

Thank you.

ALAN GREENBERG: We'll take a brief survey at the end about how many people have changed their opinion.

Two issues. The Internet breaks regularly. If you run Internet infrastructure, it breaks. If you are even a moderate-sized ISP, you have technical people who can fix things. So let's put in perspective. The Internet is highly unreliable. Routing problems happen all the time. If you're running an ISP, you find you have people around who can fix these kinds of things. So I'm not worried about that level.

Next we have Eduardo.

EDUARDO DIAZ: Thank you, Mr. Chair. This thing about the rollover is a conundrum because the mission of ICANN is to keep the DNS secure and also stable. Once this rollover comes in, it's going to be totally unstable because there will be people that this thing will not work.

I don't understand the whole process, but I think, once you change it, it has to be changed at the same time, at the same time in every time zone around the world. Let me tell you. That will, if that's the case, stop the Internet for some things.

I understand also that this is going to happen on October 11th. It's very close to, say, September 11. Well, that's what I felt when [inaudible] was going to be on October 11th.

The last thing is that I learned a long time ago that if it's working, don't fix it.

ALAN GREENBERG: But it's working and with a potential of breaking in a really serious way. Remember, if the key is compromised, no red lights go on. Suddenly things start going on and eventually you will determine that we think someone is mangling the root. Then we'll have to roll the key. So it's an unknown, and it's bad cryptographic practice to not do it.

EDUARDO DIAZ: Many people have tried to find the Coca-Cola formula. They haven't – yet – in all these years.

ALAN GREENBERG: There's not as much at stake, actually, in the Coca-Cola case. There's only billions of dollars in that case.

UNIDENTIFIED FEMALE: Sebastien.

ALAN GREENBERG: Sebastien?

SEBASTIEN BACHOLLET: My question would be, are we in the same situation as with the Year 2000 bug (Y2K)? Are we going to talk it out [inaudible] nothing happens, and then we say, "Why did we spend so much time on it?"

If I understand clearly, we need to have the DNSSEC. We have some technical skills at that level. They went up to DNSSEC, which is not that easy. My ISP doesn't have DNSSEC. It hasn't been done yet, and it's a pretty big company, a pretty big ISP.

So I believe that this is something that is not that complicated, which is not that dangerous, since the people that already dealt with DNSSEC have enough technical skills to deal with the key rollover.

Thank you.

ALAN GREENBERG: Ricardo?

RICARDO HOLMQUIST: I'm going to speak in Spanish. What I don't see is a strategic plan or a marketing campaign. I was hearing that you're saying that we're going to talk to the RIRs about the addresses that are not properly resolving. We should have done this a year ago. We've already talked to the banks.

For me, the main implementers of DNSSEC are the banks. It's those who transfer money, those who bring and take money, more than an ISP. We have already talked to the world, regional, and national bank organizations.

I don't see that there is plan from the point of view of ICANN to talk to those involved. Many of them don't know this is happening.

Perhaps October 11th – it's still a valid date – validates, as Holly was saying, with clear things in the middle between now and October 11th. I don't really see them. I don't see that they're coming here and that they're asking for our support to talk to our local ALSes, to talk to the different ISPs. That will be the users. How can we help?

At the end of the day, we will be affected. I can't really imagine a country that has three or four banks where DNSSEC is not working so they can't transfer money that day. This can cause a financial crisis in many of our small countries. This can happen, actually.

So it's not only that you're not going to be able to have access to the Internet.

ALAN GREENBERG: Tijani?

TIJANI BEN JEMAA: Thank you very much. First of all, I learned that, if you make a comment after each commenter, you will impact the decision of people. So please comment as everyone takes the floor –

ALAN GREENBERG: I have stopped and put myself in the queue.

TIJANI BEN JEMAA: Okay. Thank you. This is a very wise decision. So I'll come back to the subject. People who think that they are safe if we don't make the rollover because the rollover can make the Internet stop – I tell that they have, perhaps, more risk if they don't change the key.

You know what it is. If someone can hack your key or the DNS key, you don't have anything after that. So the danger is there. If we want to have something properly, we have to do things properly. And the technical staff/technical people said that we have to do it.

I understand that there is this problem of resolvers. This is a problem of resolvers. But there are solutions. First of all, ICANN will make an outreach campaign to make all the ISPs or all operators know that this rollover may affect the resolvers that are not up to date. It is only a software update, [inaudible].

I know that everyone didn't do it. Perhaps they will not do. But the solution – and ICANN should say that – if you are not sure of what you have, is to just turn the DNSSEC off. Your Internet will continue working. When the key is rolled, you can put it on. If you have a problem, you turn it off and you fix the problem.

In this case, you will not have a big problem. There is not a catastrophe. But if you keep the same key since the beginning – I don't how many; five years ago? Five years ago, it was planned that it would be changed yearly.

ALAN GREENBERG: Abdeldjailil?

ABDELDJAILIL BONG: Thank you very much. We talked about the KSK key, but what will be the impact for the end user in Chad that is going to connect? How can you explain that? How you can have more information about it in simple terms? If we do not change the key, if I understand clearly, it's going to have an impact on the Internet. But how many people do not have an Internet connection? Is it going to be seen as censorship? Where is the key? How does it work? What is going to be the impact?

ALAN GREENBERG: Javier, I think.

HOLLY RAICHE: Yes.

JAVIER RUA-JOVET: Listening to everybody, on the technical side, there's experts out there, and I think there's a consensus that the risks might not be catastrophic. But I think the issue here is more political. And what Ricardo said. And also what Sebastien said. Similar premises, but following on different sides of the issue.

You have Y2K. The world was going to end. Accordingly, they made a huge informational effort. The world didn't end. That's fine. The world is not going to end with the KSK change. It's not. But some things could go wrong. If you look back, ICANN said little or nothing to warn in a way that it heard – the U.S. is a bit crazy right now.

One thing we can predict is the unpredictability of some people in office. If we're going to protect the stability of the Internet, we have to protect the existence of ICANN, which could be brushed away from a minor mistake. So this is not a technical issue, really. It's a political issue about ICANN's – I hate the word "optics" – reputation and the capacity of people to take things and create crisis for their own benefit. We cannot be aiding that situation.

I think caution is required – the maximum caution possible.

ALAN GREENBERG: Hadia?

HADIA ELMINIAWI: The only risk, actually, that I see is that we haven't done it before. So we need to go ahead and do it.

Responding to Ricardo, where he said that there is a time where this key is stopped and the other one is working, there has to be a period of overlap, where both keys are actually used. So the 2010 key will be used along for signing while the 2017 key is present until the systems learn about the 2017 key. So there is a period of overlap.

But I do agree that there will be the time when one key will be stopped and the other should be used: when the systems learn about the 2017 key, using the 2010 key. So there is a period of overlap.

No, one will be used, but the other will be present until the systems are able to use the 2010 to learn about the 2017.

ALAN GREENBERG: That isn't the way it works, but we'll get to that later.

JOHN LAPRISE: I have a few brief comments. One is that, when we've spoken with the technical community and with David today, the sense of the technical community is, "Well, if it breaks, then users be

damned." He said that in no uncertain terms. I understand that from the technical community. They're technologists. We represent users. That's our primary concern, first and foremost.

With respect to risk, we're talking a lot about the potential risk of who might affected or what. But we've also heard from the technical community that the risk is unbounded. The data they have they don't understand. They don't understand why it's happening or what's happening. They just see, on the graphs they have, the non-compliance rising. Who knows where those graphs will be in six months?

With respect to the communication plan, one of the other points that was brought up by the technical community is that they don't know where the resolvers are. How are you going to craft a communications plan to reach those people and the people who operate those resolvers?

Those are my core points. I just want to reassert that, as ALAC, we represent the interest of end users, first and foremost. That's what we really need to be concerned with.

Thank you.

ALAN GREENBERG: Taking a very short pause – we still have one, two, three; about seven people in the queue. If we want to allow a little bit of time

for the discussion on metrics, then I'll close the queue right now. Or do you want to let it run?

[Penny], I'm asking –

UNIDENTIFIED FEMALE: This is important.

ALAN GREENBERG: …in general. This is important? Keep it going?

CHERYL LANGDON-ORR: This is important, Alan. This is very important.

ALAN GREENBERG: All right. Then we will keep the queue going. Olivier?

OLIVIER CREPIN-LEBLOND: Thank you very much, Alan. I think that one of the problems that we're faced with here is the number of unknown unknowns that we have in front of us. It's not more so as, "Well, it will break. Millions of people will be out of Internet connection because the resolvers will not work," etc. The fact of the matter is that the Internet is so diversified that there are many different ways in which people access the net and the kind of topology by which they have it.

Some might rely on a single resolver, which of course puts them at risk if that resolver fails to work. Some are on multiple resolvers, in which case they might see a millisecond delay in resolution.

The problem is that we don't know. So the consequences are unknown. The thing itself is unknown because you can't test it. There's no way to actually do a test network and see, if things go wrong, what will happen. So the safest solution, of course, is to try to find solutions for it.

That said, the Internet keeps on having to move forward. So you can't just suddenly say, "We're going to keep to steam engines in a car because this [inaudible] technology and the ones that use gasolines explode and kill people," because we'll stick with steam engines all the time. So you do have to move forward.

There was one thing which is a concern, of course. There's no real, exact analysis of this up to a certain point. Corridor talk appears to be amplifying rumors that the board might be asking the SSAC to look into the issue and to provide SSAC advice or an SSAC report on the issue, which will take time. The question is, how quickly can the SSAC come up with something?

I don't know if it will answer our questions, but with regards to what we should do, my personal view is that we should

definitely think of Plan B's and Plan C's. And certainly, on communication, we have our part to play.

That said, I was very disappointed with the response of the GAC that we heard a bit earlier. Also, through corridor talk, one representative came out afterwards and said, "Look, there's so many junior people here. They still need to learn a few things about ICANN." So we have admit this as well. Thus, we probably need to take leadership on this.

Thank you.

ALAN GREENBERG: Thank you. I'm next in the queue. Tijani said I shouldn't rebut. I was trying only to point out where someone was saying something as a fact which was technically wrong. But I've restrained myself.

But you'll have to forgive me now. The details are unknown, but people who have been doing this and care about it do have some pretty good ideas. We know DNSSEC has not been widely accepted. Those who have not accepted it aren't going to be impacted.

We have some moderately good numbers, though not 100% accurate on DNSSEC. When David tells me that their current estimate is that maybe 4% of people will be impacted, do we

know that's the right number? No. But I have some level of confidence that it's not 50% and probably not 20%. So it is not that unknown.

On the comment about overlap, the way it works is that the resolver allows us to insert the new trust anchor now. It is not being used. Essentially, without going into it technically, the resolver that has the new and the old trust anchor will work with either. The resolver that only has the old trust anchor will work until we change it. The moment we change it in the root servers, it's changed. So you have all of the time to install the second trust anchor – you've had two years now – but then there's a moment of truth, where either installed it and it'll work when we change it in the root servers – essentially, when we install a new version of the root, which is signed with the new key. Once it's signed with the new key, only the new one works.

So there is no overlap in the live system. It is a moment of truth.

On the question about Chad, if Chad doesn't have really good connectivity and the ISPs are doing their best to provide connectivity, maybe they haven't installed DNSSEC, in which case no one is going to notice anything.

If they have installed it and they're a really… ISP as I said before, the Internet breaks all the time – hopefully they know someone. If they've installed DNSSEC, they probably have someone on site

who can fix it. Is that 100% guaranteed for everyone? No. But it gives you a better idea.

On turning off DNSSEC, the best estimates from the experts are that, if anyone turns off DNSSEC, they're going to play it safe and keep it off. It's not a 100% rule, but that's the best guess people can make based on psychology and protecting themselves. We're already seeing, as of today, probably because of the key rollover, people already off DNSSEC [who] have it today. So it may not be what you would recommend, but that seems to be what people are doing.

On the Year2K, I oversaw a major production point at that point. Of everyone said, "Ah, it's not a problem," the world would have come close to coming to a close. Most banking systems, airlines, and the systems running your corporate business and universities had code that would not work, period. We didn't see a major problem because an awful lot of people around the world spent two, three, or four years rewriting code.

So just because nothing happened doesn't mean there wasn't a problem. It was real. It was amazing how many recently-built systems had not done it properly. Systems built in the mid-'90s were vulnerable in many cases.

On Ricardo talking to people, your point about going to banks is a really good one, I think, because central banks and

communicating banking associations are probably really good places to inject into countries. And they're big enough that they may well have their own DNS servers. There's a good chance they have DNSSEC enabled. So that's a really good point and we should pass that on to things.

But ICANN is doing a lot of talking. ISPs and people like that they are [talking] to, except that people listen to them. But not everyone listens.

To the extent, if you're in small country anyway, and you have contact with decision-makers, you know who runs the ISP, and you know who runs the computers for your local central bank, talk to them. I think we have a role to play in communicating with our ALSs, and we should use that to whatever extent we can.

Next we have, in the queue, Seun.

SEUN OJEDEJI: Thank you. For the record as well, I'm not sure that the technical points you were trying to correct when I made my statement initially – because that is the thing. [That can happen] for end users. It's actually for [inaudible] changes our resolver. That's adjusted. So the one that is compliant – so I don't know what the technical points that you were correcting there were.

Now, to my main point, we are not the technical community. We are end users. I happen to belong to the technical community as well. The technical community has given a plus-one for this. We are not the ones that fix the issues. What I would roll over on the 11th I would postpone for one year. Whatever issues that come up that are technical issues, we are not the community that would fix it. It is still the technical community that will fix it.

So I think we need to recognize from that perspective that this problem is technical. It is something that can be contained, especially if the technical community are fine with it. And we [heard] it clearly.

So I have no problem with us going the route of awareness, which is what we should do. But I'm strongly saying that we should not support the rollover. It's not our responsibility that we should [inaudible] serious [inaudible] that we want to bear because we do not have the solution to fix it if it becomes very disastrous.

IPv6 has been here for so long. People have not deployed up until now. Some of them have not deployed it. It is their cup of tea that will face when the [inaudible] starts breaking, when the networks start breaking. It's a problem. We have to do what we have to do. We can't because of certain portion of users or a certain portion of ISPs who are not responding or reacting to

changes in the Internet deny progress for those who have done [inaudible]. Because that is it. That is what we eventually do if we don't allow this rollover to happen. People [will now] be compliant. Let's reward them for it.

Thank you.

ALAN GREENBERG: Alberto?

ALBERTO SOTO: Unfortunately, I would say that I don't agree with the last opinion because we are representing end users and we need to take into account all the elements and measures being taken with being a multi-stakeholder system so that we can decide if these measures will affect end users or not.

Ricardo said that there is a marketing plan. Well, I'm not sure about that. I don't know if that marketing plan is [available] not, but I would say I'm fully sure that I talked to our RIR and mentioned that to offer LACRALO, with all its countries and ALSes, because I have the necessary technical knowledge for that. We could reach the ISPs. We could reach universities. We could reach anyone who has a data center to perform a survey because they requested from us certain help with the implementation of IPv6 because, in the LAC region, there is a

delay in this sense. So we are supposed to perform a survey for this.

I also mentioned the KSK issue, and they told me, "Yes, you can go ahead with that." But I don't have a concrete answer yet.

So I don't know if that marketing plan has been implemented or not. We were supposed to reach more than 20 countries, but nothing was done about it. So I don't know if the outreach was properly done in that sense.

Additionally, Alan said that the Internet breaks down, but if the Internet breaks down right now, it will be ICANN's fault.

ALAN GREENBERG: Bartlett?

BARTLETT MORGAN: I just want to say really quickly that fear is very, very, very bad advisor. If you have a decision to make and the primary reason for not making a decision is fear, then you're probably not using the appropriate metrics.

I'm listening to the examples that are raised in support of saying we shouldn't go ahead. I'm going through them one by one. Let's start, for example, with the banking example. Now, the proposal was excellent, but using banks as a category isn't a

good idea because, as risk management goes, for any category of persons who engage with the Internet, banks are more likely than not to have correct and credible information relative to everybody else. So they're probably not going to be the people who can't be reached by ICANN and so on. It's just an odds game.

John has raised the list from the IANA transition, but when you actually read through the list, all the markets are listed as – what's the phrase they used? In terms of basically higher risk. They're saying the likelihood is next to zero, pretty much.

Two, I also want to endorse Bastiaan's observations as well on that. But I don't want to jump into that too much. We're not here to talk ad infinitum. I just want to go through the points quickly.

There was the next point that was raised, saying, "Well, this is really a political issue. It's about ICANN's reputation. What if it goes wrong slightly?" and so on.

Okay. But then, in support of that, we referenced end users and so on. But to my mind, those are separate things. Whatever PR backlash ICANN may face isn't directly related to our role as supporting end users. That's just in a nutshell.

I don't want to through it anymore. Here's the bigger point. In my view, the issue ought not to be whether we ought to go

ahead but how ICANN ought to go ahead. Some very valid concerns have been raised so far, like the effectiveness of their marketing and their educating of the community.

For example, I don't think we as a committee are sufficiently educated on the nature of the KSK rollover to have an even more informed debate that we perhaps should be having at this point. So we can start there.

In fact, I'll stop there for now. I don't like going like going on too long.

ALAN GREENBERG: Tijani?

TIJANI BEN JEMAA: Thank you very much. Javier, I hear you. I can tell you that those who are the most aware that the transition shouldn't collapse are the American people.

You know why? Because they know that there are at least two other roots ready to run. The biggest fear they have is the fragmentation. So don't think one moment that the Americans will accept the fragmentation. They will not ask ICANN to bring back ICANN to the NTIA. This is my first point.

My second point, John and Alberto, is that it is because I think of the end users. It is because I want to preserve the security of the end users that I ask to make the rollover. If you don't make the rollover, you don't know when you may have a big problem.

If you want to have your system secure – if you have the DNSSEC, of course – you have to make the rollover.

The last point, I don't think we have to decide according to presumptions; a presumption that, if the DNSSEC is turned off, it will never be turned on, or something like this. Or perhaps that there is no technician to make this operation. Those are all presumptions, and we cannot build our decision on presumptions.

Thank you.

HOLLY RAICHE: I'm actually sitting here listening to what sounds particularly scary. As I mentioned before, in our region, there would be very few if any, who've got DNSSEC. We're basic here. I guess, in a way, for them, ignorance is bliss. Until the sky falls down on their heads, of course.

David Conrad, last year, came to the gathering of the Pacific Islands Telecommunications Association. That's all the telecom operators in the region. He gave them a great talk. I sat there

and listened to it because I was thinking, "How is he going to target it?" because a lot of the operators are non-English speaking. English isn't their first language. But he targeted his talk at a level which, really, anybody could have understood. These are technical people, anyway, so they should have understood what he was talking about. And I had a chat with him while he was there.

Not too very long ago, I had to contact him for something, and in passing I asked him if he had any feedback on people who had taken up the DNSSEC after his talk. He went and checked, and there was not one. So what do we do?

ALAN GREENBERG: Kaili next.

KAILI KAN: Thank you, Alan. Well, it seems like I'm the only person who has taken a unique position: having not taken a position. My reasoning is the following. Say somebody in my family, a loved one, is sick and in the hospital, and the doctor says he or she needs an operation. There's certain benefits and there's certain risks. As for me, what is my opinion? "I don't have an opinion. I am not a medical doctor. You are the medical doctor. You are the professional. You weigh the benefits versus the risk, and

then you decide. All I want is my family to be well." So that's why I didn't take a position: it's not for me to judge it.

Still, I'm not convinced I can take a position to judge on this issue. Still. So that is why I'm taking this position.

Thank you.

UNIDENTIFIED MALE: [inaudible]

ALAN GREENBERG: Thank you. John and I will be leaving imminently. I'm going to make a couple comments, and then I want to take a brief survey around the room.

In terms of marketing programs, I believe ICANN is doing a lot. But if you believe that you have some idea of who should be contacted, other than doing it through our own ALSes, which we don't need them to do, then speak up, because if you think you have a good idea, maybe you do.

I suggested banking because Ricardo said that, if the banks fail, we have a problem. Well, yes. Hopefully the banks are awake and paying attention, but just in case they have installed DNSSEC and haven't, it's another path of communications. It's not that we're saying it's going to change the world.

Someone made a comment – I don't remember on which side; it may have been Tijani on the "let's go" side – on presumptions. Everything we're talking about is based on presumptions on both sides. Ultimately we will have to make a decision on go/no-go based on unclear, un-full information. That's, unfortunately, life.

Okay. Before I leave – John, I know you're in the queue; maybe we want to let you go next, just to get in; the whole session only has 15 minutes left, or 20 minutes now – is there anyone here who has changed their opinion based on the survey we took initially?

Holly has changed her opinion?

A very short comment because I do have to walk out.

HOLLY RAICHE: I would vote yes, but what I said the second time around was that I would like a lot of assurance as to the kinds of campaigns that will be widespread, that will ensure that ICANN's reputation is for proactive warning and so forth and so forth.

I understand it would be a good thing, but I also understand that I would like ICANN to be taking as much as it could do. Just as you said with Y2K, there was no disaster because of what they did. If we can push that line, I would vote for yes.

ALAN GREENBERG: Okay. You may well be in a position to change.

Tijani is changing?

TIJANI BEN JEMAA: [No].

ALAN GREENBERG: Then let's leave it be. Tijani wants to be in the queue.

UNIDENTIFIED MALE: [inaudible]

ALAN GREENBERG: Okay. You have 15 minutes left before the break – a little bit longer if you want to go through the break. John and I will be outside.

UNIDENTIFIED FEMALE: [inaudible]

ALAN GREENBERG: We have a meeting out here. We can't go past the break.

John, if you want to speak quickly, and then both of us will run out.

JOHN LAPRISE: I just want to add a little bit of nuance for people to understand my position. Yes, I'm saying no to the rollover at the current date. What I would like is for, on the technical side, the data be better analyzed because, right now, the technical community is not understanding what they're seeing in the data flows. So I want better understanding there. And I would like a better communications campaign prior to the rollover.

Thank you.

HOLLY RAICHE: Okay then. Off you go.

UNIDENTIFIED MALE: [inaudible]

MAUREEN HILYARD: Okay. We'll continue on with the queue if people want to do so. We've got Daniel [inaudible].

UNIDENTIFIED FEMALE: [inaudible]

DANIEL NANGHAKA: I'll assume I don't understand much about this whole thing, but it looks like there is fear of what is going to happen to the Internet. Whether they like it or not, at a certain point in time (T), they're going to make the rollover.

The end user needs to the Internet, which is a constant factor, but what about in case the rollover doesn't take place and the Internet breaks? What will happen? Those [too] go back and complain.

So my opinion is, considering all other factors constant, the technical community already understands the risk of the future. Then let's mitigate the risk. Make the rollover. Those ones who haven't updated their systems will go ahead and do it because they'll have to fight back their clientele because this is where the business is.

Thank you.

MAUREEN HILYARD: Sebastien, did you have your [inaudible]?

SEBASTIEN BACHOLLET: Thank you. Just a point. In parts of the world, you have more than one provider to be connected to the Internet. You use

something for your phone, something for your laptop. In the other countries, where you just have the phone, there are usually two or three companies over there. Then it's not so much [that] we can't contact them directly to be sure that those phone companies are doing what's needed to be sure that end users have access. Therefore, I think that their mitigation is the way to mitigate the situation.

Don't forget that you just have one single item to connect to the Internet in large parts of the world.

Thank you.

MAUREEN HILYARD: Thank you. Javier?

JAVIER RUA-JOVET: Thank you, Madam Chair. On the point of whether or not this is of the interest of the end users, I understand that this varies a lot from region to region. Puerto Rico is an early adopter of DNSSEC. .pr is like the third in the world, and others have followed suit. So it matters to the end users that are close to me.

Thank you, Tijani, for answering me directly with your opinion. [Adam] talked about presumptions. I think what you said to me is presuming a world where geopolitics are run by adults and

that geopolitics are run on national interests. Trump is crazy, and he surprises his closest staffers. Imagine the civil service and the adults.

I know nothing or next to nothing about the technical aspect of this, but I know what U.S. politicians from the right want to do with ICANN. Trump will do whatever he feels like that morning. Forget about presumptions.

That's it.

MAUREEN HILYARD: Thank you, Javier. Narine?

NARINE KHACHATRYAN: Thank you very much. My perception was that the process of the DNSSEC rollover can be stopped at any time. Isn't it technically possible to stop it if something happens unexpectedly?

Thank you very much.

MAUREEN HILYARD: Thank you. Holly, do you want to say anything more? You were in the queue.

HOLLY RAICHE: I think it has all been said. I think I've made it clear, and picking up the point that Javier said, I think it's really important that there is a very widespread, visible ICANN-and-others' publicity campaign. I think there has to be a lot of understanding, as much as possible, about the risks. I understand the risks of not going ahead. I think that, with any comment we make, we must reflect our reservations. We must, in fact, say we're disappointed if we have to actually turn off DNSSEC because it's a security thing but point out that, actually, our concerns are really with the end users. I think there's lots of things we have to say if we're going to say yes.

Thank you.

MAUREEN HILYARD: Tijani and then – no, no, no. [Then you. Go ahead].

TIJANI BEN JEMAA: Thank you. I heard several times people saying that we don't know what the resolvers that may have those problems. So to whom will we reach out? This is not a problem at all. Those are not end users. We are speaking about providers. All the providers have contracts, and contracts go [until] ICANN. So you have a reseller or – I don't know – a register and a registry, etc. At

the end, you have ICANN. ICANN has all the records for every one of those operators, and it is easy to reach out to them.

We are not talking about our end users. Yes, you have to know to whom you have to go. If there is a complaint, it will be a complaint for every operator. This is the only way the campaign can be done.

Second, Alan said that everything is based on presumptions. I will repeat what I said. Tell me what the presumption is. I said that, if we don't make the key roll over, we have a big problem because we have already five years with the same key. To hack the servers is something that a hacker can do. When you have your server hacked, you will be in big trouble. This is not a presumption.

Third, I said to do the rollover. How do you do it if you don't have visibility and you are really frightened? Go safely. Ask everyone who has DNSSEC to turn it off. Make the rollover. Ask them to turn it on again. If there is a problem, the one who has a problem should turn it off, fix the problem, and then turn it on. What is the presumption? No presumption.

Thank you.

MAUREEN HILYARD: Thank you, Tijani. We've only got a few minutes left. I've got Alberto, Olivier, and Satish. One minute each.

CHERYL LANGDON-ORR: And then we do some…

ALBERTO SOTO: I have been working for more than 30 years in IT, and for more than 20 of those, I've been in charge of the full responsibility of the IT area with the implications in security.

I've heard the word "fear" three times here. Not being afraid is not being brave. I've never been afraid. I've always had the responsibility of doing what you have to do in IT, which is risk analysis. Risk analysis is not the same as fear. I do a risk analysis with a certain amount of information. And the information that I have is not enough. It's just not enough.

If the technical area in ICANN would provide me how it is they got there and what the presumption is, there will not be many end users who would suffer. If there will be a certain Plan B or C or D, or there will be a certain regulation, then I would vote yes. But so far, with that presumption, and with the warnings that I have, I will have to say no.

Thank you.

MAUREEN HILYARD: Thank you, Alberto.

CHERYL LANGDON-ORR: Olivier.

OLIVIER CREPIN-LEBLOND: Thank you, Maureen. I wanted to respond to Narine Khachatryan's question regarding being able to roll back; if you decide to start the rollover and then say, "No. It's not working. We can stop it." I know that Cheryl replied, but she was off-mic. The answer is no, you cannot. Once you've started, you can't back because you'll basically end up with some systems that will continue moving forward and other ones that might roll back. It would be more of a mess than just continuing forward.

MAUREEN HILYARD: Thank you. Satish. That's the end of the queue.

SATISH BABU: Thank you. A couple observations. One is that I support the rollover. That is a clear thing. But there are both technological and political fallouts that can happen. The technological fallouts are actually not that serious, according to my estimates.

The political fallout? Tijani mentioned two countries ready with their roots/ I know one country, at least – I don't know which the second is – that is ready with its alternate root if this gets out of hand.

I run the [inaudible], and I run a resolver on my laptop. Many wireless access points, for example, run resolver. Most of them do not use DNSSEC, so they're immune to this. But we must have an estimate, either by simulation or by some other study, of what percentage of the Internet is under threat and whether this number that we hear is really realistic.

Well, Seun said it's impossible to do that, but I'm not so sure. Maybe ICANN can make an insulated sandbox kind of place where they can test out this sort of thing.

I'm scared more of what Javier was talking about in terms of the political fallout, especially given that, one the one, we have Trump, and on the one hand, which are ready with their roots. So that kind of situation is what scares me a little more than the technical part.

Thank you.

MAUREEN HILYARD: Thank you, everyone. I think we've had nearly 90 minutes of really fantastic discussion here. In fact, I have learned so much

about the whole – I didn't go to the last session. We were busy talking money. I'd like Cheryl do a summation because you wouldn't want mine.

But one of the things that I would like to get is that we actually come up with some summary/summation. We'd probably need to find a penholder. I'd really like something to come out that we can actually present. There are so many great ideas – the marketing, the need for more communication, more information [given] between now and October if that's the way they're going to go.

So I'll leave it to Cheryl.

CHERYL LANGDON-ORR: Thank you, Maureen. This is one of those rare occasions when 'm actually struggling to remember a more fulsome and fascinating discourse around your table. So congratulations. From my observer status, you have had a very productive and very useful conversation.

I suspect, however, if I've heard correctly, that it's a conversation that's not ready to be concluded yet, that there are some what-ifs, buts, and maybe's not be considered. Based on what Maureen was saying just then, perhaps if we have one or two people consolidate what we believe we think we have heard,

some notes have been taken and put it up on a wiki page while all your juices are going and while you're as passionate about this subject as you clearly are and need to be, let's see if we can progress this to a white paper for, at least, discussion.

I've also heard a couple of needs for clarification. I've also thought a couple of times that one of thing to perhaps ameliorate the potential political fallout, if we cannot, as someone pointed out, get to the people doing the resolving because we don't know where those resolvers actually resolve. Why not prepare and have ready to go a very professional and aggressive PR exercise to minimize an effect on ICANN? There's probably some smart ways of thinking.

With your permission, I'm going to propose to you all that we have – obviously, I think Alan is quite passionate about it – someone on the counterarguments and maybe ask Javier to hold the banner on the "I'm very cautious" side of things. Maureen has made some notes. If anyone would like to give Maureen their name to help with, perhaps, Hadia, that would be perfect. So you've got Hadia, at least. This would just be a rough little drafting exercise, and then you all get to work on it with the wiki.

Sebastien, over to you.

SEBASTIEN BACHOLLET: Thank you, Cheryl. Just one point. There were three names on Skype who said they are willing to take the [pen]. Maybe it's a good way to take them. I guess Baastian will write something. I guess Seun and Aida could but that's just my –

CHERYL LANGDON-ORR: Thank you. Of course, this is not penholding the document. This is drafting a precursor. If you then decide you're going to draft a comment, you still need drafters for the comment. Let's then work out a time. Maureen will get in contact with all those people and let you know when, during this meeting, you're going to have to make time to start putting that first case together.

Can I ask you all to, as we usually do – there's another meeting in this room when?

UNIDENTIFIED FEMALE: Now.

CHERYL LANGDON-ORR: Now? Okay. Can we clear our spaces as quickly as possible? Thank you, one and all, for a very productive meeting.

MAUREEN HILYARD: Thank you, everybody. We better move, I think. I will meet with Hadia, Seun –

CHERYL LANGDON-ORR: Grab them and take them outside.

MAUREEN HILYARD: Yeah. Hadia, Seun, and Baastian.

[END OF TRANSCRIPTION]