SAN JUAN – ALAC & Regional Leaders: Work Session, Part 10
Tuesday, March 13, 2018 – 11:00 to 12:00 AST
ICANN61 | San Juan, Puerto Rico

ALAN GREENBERG: We are one minute after starting time, can I ask staff to try to round people up from outside?

Can we please have At Large people seated? Since we don't have the NomCom staff here yet, there's another issue we need to discuss. Maureen and Ali? Olivier, Eduardo, before we start the formal meeting, after this meeting we have the ALAC meeting with the GAC, but in parallel with that is the discussion on the budget and operational plan. And, I like to take a quick poll of who plans to be at the GAC meeting, and who plans to be at the budget and planning meeting? I don't think we can afford to skip either.

Well, I have no choice but to be at the GAC meeting. Okay, everyone who didn't put up their hand is at the GAC meeting, thank you. It would be nice if we had a few ALAC members with me. As long as we have roughly a split 50/50 on ALAC members and regional leaders, I think we're okay.

Do we have any input from NomCom staff where the NomCom leadership is? I see a number of NomCom members in the room.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

UNKNOWN SPEAKER: Today the programs are so packed, probably they have the previous meeting conflicts with your meeting.

ALAN GREENBERG: I understand, but we have another speaker coming afterwards on a rather critical subject, so we're not going to be able to run over the time. This was described with NomCom leadership with us, I don't know if they have the pitch, but if any NomCom member here would like to speak, I'll be glad to start the meeting if the recording is started? Can I have confirmation that the meeting is formally started, and the recording is started? Yes, I see someone with a hand way back there. Please, go ahead.

SANDRA HOFERICHTER: Sandra Hoferichter speaking from the NomCom, we have a WHATSAPP group, and I was asking where they are, and they said they're running late and leadership will be here shortly, but I think in the meantime, as various NomCom members are in the room, I see Nadira, I saw Haziz, is he still there? And myself, and we also have our review team. Maybe we…no, you're not from the review team? Sorry, I mix faces. So, let's either skip, change the agenda, or make use of the people in the room.

UNKNOWN SPEAKER: Please go ahead with whatever you can. I think in the vernacular; fake it. Whatever you can.

SANDRA HOFERICHTER: Since this is my community, the ALAC, and I'm very happy to be back, and I'm also a second-time member on the NomCom, I take the guidance from my former chair. So, as I said already, it's my second time of the NomCom, and this meeting in particular, interesting and important for us to do outreach activities. The current numbers of applications, which we reviewed—oh, and I see my chair is arriving.

The current numbers of applications we received need to be improved, and especially we need to have much more applications from the Latin American region, and I would like to encourage all the people in the room, and in particular those from the Latin American region to set up an application. You will still have time to do this until the 19th of March, just to say, "Hi, I'm interested," and then you will have another week until the 26th of March to complete your application.

And with this, I see that the leadership team has arrived, I'll hand over to Zahid and—and I just finished that sentence, so there was nothing else secretly I could explain.

ICANN 61
COMMUNITY FORUM
SAN JUAN
10–15 March 2018

ZAHID JAMIL: Thank you so much Sandra for doing that. I really appreciate it because we were running late, coming from another meeting. You can imagine there's a lot of conversation about us, so we're having to answer a lot of questions, that's why. Why don't I let you decide how you would like us to proceed further?

ALAN GREENBERG: The meeting is yours, but at this point, officially it ends in 10 minutes, but we can go a little over, but we have another speaker and a relatively critical issue to discuss.

ZAHID JAMIL: Can we go quickly through the slides if you're got our slides up? Who's managing the slide deck? Next, next, next, next, next…oh, you can do this, can you? Perfect, thank you so much. So, I won't waste your time with what we look like, and I believe Sandra has explained the slots that are open in the ALAC, if anybody else knows exactly what these things are, three board, one GNSO, two ALAC, which are geographically mirrored and two ccNSO seats.

One thing I wanted to clarify, which we realized doesn't actually socialize; you don't need recommendations from these groups

to apply for these groups. You don't need to come from these groups to apply to these groups. And, the funny thing we heard from folks is, "Well, I didn't apply for the GNSO because I've got nothing to do with the GNSO, they won't recommend me." I was like, "No, not at all, you can be anybody and apply to this," which is something that I think is important—we thought it was understood, but I guess it bears repeating.

As you can see, last year we did very well, we went from 19% women who applied to 36% of women who applied last year. Our numbers this year haven't come in, we're hoping for better numbers this year, but as you can see, we're making year on year progress thanks to many people, especially the DNS Women's Cocktail, many of the other events that take place at ICANN, and a lot of the ladies who actually worked last year based on the hard work HP did, he's our associate chair and chair from last year, to make sure that the numbers in that really increase.

And, you can see that the positions we filled from 29% went up to 50% as regards to women last year, and hopefully we're going to do as well if not better this year. Yeah, 50% is a good number, you're right.

Now, you've seen what's up there, and we notice that, excellent, it's March 2018, somebody fixed that, thank you. We had a type-

o on that screen. So, you can see that now we have for the first time a constant website called NomCom.ICANN.ORG; we used to be ICANN.ORG/NomCom2016, '17, '18, '19, '20, and so Google Search was a disaster with that, so we changed that. And by the way, you can suggest people, if you think that someone who's useful, and you'd like to send us a name of a person we should reach out to, please do that in the last link below. Now, very quickly, what I want to do is talk about the improvements we had this year.

We've noticed that we have great responsibility, but no power to some extent regarding our own operations; we noticed that the NomCom's destiny seemed to be pre-determined before it's birth, and that we had a Groundhog Day because we couldn't fix this every single time, every year we were confronted with the same problem. At least the five years that me [inaudible] have been on.

And so, we couldn't basically do anything else but hire the same recruitment firm, or not have a recruitment firm every single year. Our budget was unknown to us, we had no idea what a budget looked like, we didn't know line items, and we had no control over the budget because staff would make the budget 11 months in advance before we were birthed, so we had no control over it. The assessment firm also; we couldn't choose,

ICANN
COMMUNITY FORUM 61
SAN JUAN
10–15 March 2018

except we had one choice; you take that, or you leave it. Our schedule, how many meetings, how many face-to-faces we wanted to have were not in our control, so basic operational planning was completely out of the hands for the NomCom and that's basically partially a bi-law problem, because by the time we actually see it, it's too late to make those decisions a year in advance.

So, this year we implemented certain improvements; on our birthday, we took all the decisions literally on that day and communicated them to staff. So, we didn't wait for weeks to do that; literally on the first day, we try to be as efficient as possible, I don't think we can be more efficient than that, literally the first that we see it, we pre-planned, we pre-discussed and we took decisions then. We forced a partial budget reveal that gave us some numbers, some interesting numbers about what different services we were getting, how much they cost, and we tried to find money within that budget; this is important, it wasn't additional money, but money within that budget to be able to do some new stuff.

So, we changed our assessment firm, we have now decided, and let me sort of give you an example of how we used to do selections; initially what used to happen was folks who were on the NomCom would look at the application that used to come in,

100 aud or whatever, and would online rate them, so 1-5, if I liked Candidate Mr. X, I give him a 4, if I like Candidate Y, I give them a 3, and we'd do that sitting at home on our own, and that led to a number; that number then led to a cutoff, and what usually ended up happening was based on that rating mechanism or polling as we used to call it, folks who fell below that cutoff number would not be considered as much as the ones above that number, naturally speaking.

You could pull people up if you thought they were interesting, but really not every candidate was evaluated in the same way, so we changed that, we said this year we're going to look at 100% of our candidates and we're going to discuss 100% of our candidates. And, we're going to do that, we're going to do the ratings still, but that rating is not going to eliminate people; it's not going to lead to a number which is arbitrary, and we cut people off. So, every single candidate who applies is here, no matter what their criteria is, we'll get consideration, full consideration, face to face meeting with the NomCom, and that's a big change; let's see if it works, but that's something we're trying to test out this year.

And there's a lot of enormous cooperation from staff in order to make that happen. We have for the first time a job description, which has been approved by what we call the experts, i.e. the

board itself. So, we sent what we thought would be the job description of a board member, sent it to the board, they made the edits, sent it back, took a while, and I think we have—and it's online now, that job description so you can see when people apply, this is not just what we think the board requires, but what actually the board feels that this is what their job looks like.

We also decided to create criteria before we get the application, so we're not building criteria based on the applications we receive and so the job description was one aspect, quality and skills that Johnathan Cohen, who is in the audience here and his team work really hard in setting together. So, there's a lot of work this year, in the last four months we've done, even before the applications came in, very hard work that our committee has done, so we have now a list of qualities and skills, and we have the board guidance we receive every year from the board, and that basically is the criteria we're going to select against.

Now, instead of survey monkeys, we are doing deliberations as I have mentioned. We are actually going to be doing proper face to face, and we've had some tech problems so even online calls where would otherwise deliberate were such a challenge, especially last year, where just to give you an idea; one third of the call was stuck on, "Can you hear me? Can you hear me? Hello? I can't hear you, hello? Are you sure?" That was the

problem. And that was 1/3 of the time we wasted on the calls, literally. So, because it's only us who is having this problem, we call it the NomCom ghost. It is specifically just a NomCom problem.

Anyway, so we're going to change that, hopefully this is not going to be a problem this year with these face to face deliberations. We've doubled our recruitment capacity, and we have a long terms strategic plan for RRSP's for a pool of recruitment and assessment firms from which we're going to be able to pick, and that will be Damon next year, he'll have the ability to do that because the RFP process is taking place this year.

Everybody used to call NomCom as a black box; well this year we're going to have at every single stage, people who are in that process are going to receive an e-mail telling them where we are in that process, and so sorry you didn't make it to the next stage, but you know, we may come back to you or whether you should apply again or not, and there's a personal commitment I've made for those who are in the advanced stages; they will get a personal call from me, the chair, or others who want to join me to actually talk to the candidates so that if we want them to apply again, or we thought that they should be encouraged, they don't feel let down; that's the biggest problem that we've heard

about the ability of the NomCom not to reach out to its candidates.

We want to know our customers; we've had training, so me and GNSO, I know nothing about the ALAC, so we had training done so the ALAC would explain to us what the ALAC is like and the GNSO and the ccNSO and vice versa, and also board governance training, and confidentiality training, and also yesterday training on how to do a good interview, or to assess an interview. All of this is being done this year. We did have interview training in the past; I think this year we've brought it back.

And there was a cart before horse problem; it happened last year where we used to make our final selections as if we were due in Panama this year, and once we'd given those names in, it would go for due diligence as they normally do. But what happens if the due diligence comes back and says, "Sorry, this person can't go through." What do we do then? No one is interested to come on a call, we're not meeting again, we can't do the selections again easily, people are just busy doing other things, it becomes really difficult, so we decided, no, we're going to have due diligence for all the people who are going to come to Panama this year prior to them coming to Panama, so when we make our decisions in Panama, we're done; there's no further evaluation selection, the selection is done.

We're not going to be a Nomad website anymore; we're going to have a standard, static website, NomCom.ICANN.ORG, and Nomad might be a good one to go with, yes. And then we're asking every single AC and SO, we put this in our operating procedures, which wasn't there before, saying we need to ask for guidance, so the ALAC would have received a letter and sent a response telling us what they are looking for in the people we appoint, the same is true for the ccNSO and others.

And we're abiding by the bi-laws of ICANN to make sure that term unlimited liaisons don't vote in the process, but they basically participate, deliberate, and they've never done that, they 've never actually voted. But what we're doing is at every single stage when a person goes from stage 1 to stage 2, that person is eliminated. The fate of that candidate is decided only by the voting members of the NomCom.

And as I know this one has generated quite a lot of question in the audience, in the community, let me be clear; the first rating, non-voting liaisons are included to do that, and the numbers are seen. When they come onto the call, the first call that we ever have, the bar is really low, they'll be a proposer and a seconder, and non-voting liaisons can suggest people for those proposers and seconders to then take that person through to the next round.

When you come to the intersessional, they will be participating in every conversation, every deliberation, and also in the straw polls; I repeat, also in the straw polls because there's word going around that they will not be participating in the straw polls. So, they will be participating in the straw polls, but when we make that final decision with that one stage where the person A, goes from stage 1 to stage 2, after the straw poll has been conducted and further deliberations take place, then that person, then that vote is going to be only with the voting members, and that goes on and on.

And also, in the interview, then the deep dive teams, which you know fairly well Cheryl, they're going to be participating in the deep dives and making recommendations about that individual who is actually evaluated in the deep dives.

And I've spoken too long now, I can see that Alan wants me to stop, so, thank you.

ALAN GREENBERG: I have one question; I think I heard you say the decision, the actual decisions of who will be selected will be made prior to the meeting in Panama, is that what you said?

ZAHID JAMIL: The due diligence analysis regarding the people who come to Panama will take place before they come to Panama so that after we select them, we aren't told by legal that, "Uh-oh, this person has a criminal background," or something.

ALAN GREENBERG: But the selection will be done in Panama? We have been requested to select our RALO ALAC members prior, so you at least know what regions they're from, and our target is to have done that by Panama, but not necessarily a lot before.

ZAHID JAMIL: It is very important that when we're in our selection process that starts basically sixth of April, it goes from sixth of April up to Panama, so if you give it to us just before Panama, it's going to be unhelpful because we might not have the people we need to appoint, because those slots are taken regarding geographic diversity. So, the sooner you can have this done; we can't force you to do it, but the sooner you can have it done, the better it is for us, but we will live with whatever you give us.

ALAN GREENBERG: Well, we certainly will not have it done by the sixth of April, the exact date to be determined.

ZAHID JAMIL: Sure.

ALAN GREENBERG: Hans?

HANS PETTER HOLEN: You may want to consult with the bi-laws, because you're actually required to make that appointment sixth months before the AGM, which is done roughly 20th of April.

ALAN GREENBERG: That's for the board.

HANS PETTER HOLEN: For the board, yes, okay, sorry.

ALAN GREENBERG: We're talking about ALAC selections.

HANS PETTER HOLEN: Okay, no problem.

ZAHID JAMIL: Can I just say something? Thank you for clarifying that Alan; it doesn't matter actually, because your slots are geographically specified, so it doesn't matter.

ALAN GREENBERG: Yes, but traditionally we have tried to avoid having two people from the same country within the region, and that does matter. Yeah, go ahead?

UNKNOWN SPEAKER: The other advantage of doing the due diligence beforehand is that you'll get the results either in Panama or shortly thereafter, there won't be the Panama meeting, and then approximately 2 and half months before results release.

ALAN GREENBERG: You plan to announce your results soon after the Panama meeting instead of August, September, October, okay.

UNKNOWN SPEAKER: So, we can't announce our results ourselves, because we're new to bi-law changes, we need to send to EC, and then that then sends it to the board, and then it's announced, but it's really then up to ICANN org. to announce it when they do. But we will

be sending our list in basically right after Panama, right in Panama at the end of Panama.

ALAN GREENBERG: Again, you're conflating the board selections with the other selections, which don't go through the empowered community.

UNKNOWN SPEAKER: So, we're trying to be consistent, so we're not just going to just reveal only others and not the board; we want to do it together, that's why.

ALAN GREENBERG: No, I understand, I'm just making clear that we have the words right. Hans?

HANS PETTER HOLEN: Yeah, so the mechanics after we have made our decision is that we go to the candidates and tell them that, and then they finally accept, so that could take days or weeks. Hopefully it won't, since we will do it immediately after Panama, they will still be in the mood that they remembered they applied and for what reason.

ALAN GREENBERG:	It happens to affect another decision we're making, so let me be really clear; you are saying we will know the ALAC appointees from the NomCom relatively soon after the Panama meeting, as opposed to two to three months later, without being specific on the date?
HANS PETTER HOLEN:	Yes.
ALAN GREENBERG:	Okay, thank you, that does change a critical issue that we have to resolve, specifically that I'm leaving, and we have to appoint a new ALAC chair, and the question is whether the new NomCom appointees are eligible or not; if we don't know who they are, they are not eligible.
UNKNOWN SPEAKER:	Just as a matter of—I'm trying to be safe of this issue, I would say, wait about 2, 2 and a half weeks post-Panama, but it won't be longer than that.
ALAN GREENBERG:	That's not critical. Do we have anyone else? We are a little bit over time, we did have a tiny bit of fudge factor in our next

session, but we've now used that up, but if there's anyone else who has any comments to either NomCom or ALAC or Regional Leaders, please? Good luck. And I understand David Conrad is in the room somewhere? There he is.

And it is with great pleasure that I welcome David Conrad. David and I have a bit of a history, going back 20-odd years, so I'm always delighted when we have him as a speaker, and I will not do a lot of words, but it's over to you.

DAVID CONRAD: Thank you Alan. And I apologize if I start coughing or anything, I seem to have picked up a bit of a cold. My voice is now better than it was this morning when I had to talk to the PSWG. So, thank you for giving me the opportunity to speak about the KSK role.

And, I suppose this technology might actually work. Okay, so, for a little bit of background; when we signed the route in 2010, we promised the community that we would roll the key, that is, change the key after five years. And, we started the process of rolling the key, thank you, in 2013, and then sort of suspended that a bit because of a small event known as the transition of the IANA's functions contract, we thought it might be better to not throw all of the cards up at the exact same time, and instead

throw them up once and then later on throw up the second set of cards.

So, when I rejoined ICANN in 2014, we did some preliminary analysis and sort of restarted slowly the KSK role, eventually started picking up steam, and then moving along quite rapidly until about September 2017. In that month, Duane Wessels at VeriSign who had published an Internet draft, an RSV, originally published in April of 2017, first got implemented in one name server in August of 2017.He started noticing data from hat implementation, the draft, standard that he'd written that was indicating some surprising data.

We had anticipated that by that time, by September of 2017, we would not be seeing resolvers that were only configured with the trust anchor that was built in 2010, but instead we'd be seeing both the 2010 trust anchor, and the 2017 trust anchor, which would mean that those resolvers would be able to change to the new key without any interruption of service.

But, at that time in September, Duane reported that he was seeing between 7 and 8% of the resolvers that were reporting their key to be configured only with the 2010 key. And, if we had gone ahead as originally planned, which the plan was to start using the new key on October 11th, 2017, then that would mean that the 7 to 8% of resolvers that we knew about would be

unable to resolve anything; they would immediately start failing and all the users behind those resolvers would be unable to look up any names on the internet.

Thought that would be sort of a bad thing to happen, so as I was just about to go on vacation, because I was definitely going to take a vacation when we're about to break the Internet. I was actually at O'Hare Airport in the lounge and I told Matt, "Okay, so maybe we shouldn't break the Internet today," and we decided to postpone.

So, we started looking more closely at data from the route servers that we have access to the data from, so at that time we were collecting data from the B, D, F, and obviously the L route servers, and just started looking at what we were seeing in addition to what Duane was seeing, and we were getting a slightly lower number than Duane; about 4.1 percent, but it was still higher than we anticipated. We were expecting less than a half of a percent, so we postponed on the 27th of September, so we could try to figure out exactly what was going on.

We started looking at the data October through December, and since we had the IP addresses of the resolvers that were reporting this information, we went and hired somebody to go and contact them. So, what we discovered was the information in the WHOIS database is not actually as helpful as one might

ICANN 61
COMMUNITY FORUM
SAN JUAN
10–15 March 2018

hope. Just finding, when the only thing you have is an IP address, finding then the operators of those IP addresses is actually quite difficult. Of the 500 IP addresses we were only able to get a response from 20% or about 100 addresses, 100 operators for those IP addresses to ask them what was actually going on. It turns out that of that, those 100 addresses, 60% were actually in dynamic addresses.

Now, it doesn't make any sense at all to have a resolver on a dynamic address; the whole point of a resolver is that's an address that clients can send queries to in order to get a response back, so that caused us to scratch our head a bit. 25% of the addresses were from resolvers that were known to be forwarding for other resolvers, so that means that there was a chain of resolution going, so for example, I could configure my laptop with a resolver and point it to Googles 8.8.8.8.8, so the only address that we would see at the route server would be the 8.8.8.8.8. address, not the actual resolver on my laptop.

We weren't able to find a single cause, which was sort of positive and negative. The positive part is that there wasn't an endemic problem with the KSK rollover plan that we had had, the software did mostly what it was supposed to do for 95%, it was a positive, but that also meant that we couldn't actually remedy

whatever the situation was, because we couldn't find out what sort of the consistent problem was.

That left us with no obvious path forward, and in general, anytime ICANN finds itself without a path going forward, we basically throw it to the community, and that's what we did. We decided to solicit the community for input, we spoke with, we had a mailing list of people who were interested in the KSK technical folk, so we sent a request for input and discussion on the acceptable criteria for proceeding with the KSK roll. There was a bit of discussion, maybe not as much as I would have liked, but there was quite a number of messages that are all archived if you're interested in the discussion.

The results of that discussion was essentially that, well, there's actually no way that we have currently to measure the number of users that are impacted. We can get a bad but useable idea of how many resolvers are not configured correctly, but that doesn't actually tell us how many users are behind those resolvers.

For example, we can see, well in theory, Google, 8.8.8.8 as a resolver, but that doesn't tell us how many people are actually using Google's resolver, so that means that the data that we're actually collecting, this 8145 data, which I have to say, the fact that we got any data out of the RFC 8145 implementation that

Duane Wessels had written was actually surprising in and of itself because the standard was only created in April, or the first draft of this standard was only created in April and it was only first implemented in August.

So, the fact that we were actually getting any signals at all out of that was actually quite surprising. But, as we move forward, we're getting more and more signals, but it still doesn't tell us actually anything useful, it just tells us that some numbers of resolvers are configured badly, what does that mean? Well, it means that somewhere between 0 and a huge number of users could be affected if we did the rollover.

There is a belief within the technical community that there will be better measurements in the future; there's a new standard out called KSK sentinel, developed by Jeff Houston at AP NIC, and that would give us actually more information, but it's not available yet, the standard isn't even finalized yet, there haven't' been anything but prototype implementations to date.

The consensus on the list was that we should move forward with the roll. The data that we're getting isn't telling us anything useful, we've always sort of known that some people will get impacted by the roll, and when I say "impacted," it means they'll be unable to do any resolutions until they turn of DNS SEC, and

the technical community's response to that was, "Well, they're broken, they deserve what they get."

As such, we are working on, and the community also said we should continue to try to contact these people to tell them to fix their configurations so that they aren't broken, but we've been doing that now for about 2 years, and have not been able to obviously impact everyone, make them aware of the fact that the key role is happening.

So, on the first of February we published a revised plan, a draft plan to proceed with the KSK rollover, with the date, which might look a little familiar; 11, October 2018, so exactly a year after we had originally planned on rolling. We within the draft plan did not provide any specific measurable criteria to determine whether or not to stop or move forward with the roll, because the community didn't actually provide us anything. We will continue to do extensive outreach, trying to tell people that if you don't fix your KSK, you will no longer be able to resolve, and are publishing the statistics more frequently.

The public comment for this draft plan is currently open, and we are encouraging everyone who has interest in this to please, please, please provide input. So far, the input we received has been almost exclusively from the technical community, and the technical community gleans that we need to move forward to

roll the key, so we would like to get a broader, inclusive input from other folks, their views on this particular topic. The public comment closes on April 2nd, so please if you have interest in this, please provide input.

That proposed schedule is on the 10th-15th of March, we will hold a community feedback session, so we will actually be talking about this in great detail. In mid-April, we're going to publish a report based on the public input, anticipating any changes that we will be making to the plan. We will provide that to the board and request a board resolution to ask SSAC to review the finalized plan by the 1st of August. We're planning on doing another community feedback session in Panama, hopefully by August we'll receive SSAC feedback, revise the plan as necessary, mid-August publish the final plan, on the 14th of September request a board resolution directly in ICANN org. to officially move forward with the roll, and then on October 11th actually do the roll.

The part of this is to just make sure there is a clear paper trail in the event that bad things happen, that there is a clear understanding that this was directed by the community; it wasn't just me deciding one day that it would be fun to break the internet, because as much as I would enjoy doing that, it probably wouldn't be career enhancing. The intent then is to

actually have full community input with a board resolution indicating that we should move ahead on 11th of October.

Just for more information, with the 8145 trust anchor reports, we're seeing data now from 11 route servers, the earlier data that we'd looked at was from only 4 of the route servers, P, D, F, and obviously L. We're using a package that Duane Wessels at VeriSign had written to actually do the analysis of this, and this is what the data sort of looks like.

So, back before January, we were averaging about between 5 and 8% of the resolvers announcing 8145 data, saying that they were configured only with single key. In January, that percentage jumped up significantly; it's now on the order of 20-25% of the resolvers say they are only configured with the 2010 KSK. That means that when we start signing upon 11th of October of 2018, that 20% of the resolvers will be unable to resolve anything.

Why was that big jump in January? Our best hypothesis to date is; there was a bug in a popular name server that was completely unrelated to the KSK roll; it was just a security fix that needed to be made to that software, so a lot of people went and updated their software. Remember these 8145 implementations is very, very new, and it's only implemented on a small number of resolvers. By far, the most common resolver on the Internet

today is Microsoft's DNS, and Microsoft's DNS does not support 8145, so we're not seeing any announcements from Microsoft, so we're not seeing any announcements from the majority of resolvers. The only resolvers that we see are folks who are early adopters of the open-source implementations, one of those is unbound.

So, when that fix went out, people updated their versions of unbound, and all of the sudden we see a pretty big spike in the 8145 announcements. You know, why are we seeing such a large number? Well, again, we actually don't really have a good idea. We've tried a number of ways to try to track down what these resolvers are, there is some hint that it might be sort of test resolvers within virtual machines that people set up just to run a test of software, and it's purely a femoral, it'll go away, and if it does fail, DNS SEC validation it won't matter because it's just for test. But, we aren't certain.

This pie chart gives you a bunch of graphs; the important part here is, if you look at the black line, it shows you that pretty much everybody is seeing sort of the same numbers, although for reasons that we don't fully understand. VeriSign is seeing less numbers than everybody else; don't know why, this whole DNS thing is black magic as far as I can tell.

One question we've gotten is; how many addresses are we seeing that are reporting, and this graph actually shows over time the number of reports, and these are in the number of unique IP addresses that we're seeing at the route servers, and it used to be pretty low and then around January it spikes up to between 14 and 1600, that's unique IP addresses per day, and if you look at cumulative over time, you'll start seeing that these numbers are growing quite rapidly, we're up to around 750,000 unique IP addresses that are resolvers that are hitting the route servers with these 8145 announcements.

Just a little more, another way of looking at the same data; these are within net blocks that are 256 individual IP addresses, so it indicates that some of these addresses are bouncing around inside a single net block, which would indicate it's dynamically assigned and therefore unlikely to be particularly worrisome should we actually do the KSK roll.

Another version of the same data. So, this is a lot of addresses; 267,000 addresses are indicating they are configured only with the 2010 key, these are the ones that will break when we sign with the new key in 11 October of 2018. There are another 464,000 that are actually configured correctly, so that's a bit worrisome, and one of the reasons I'm encouraging people to

provide public input during the comment period is to let us know how they feel about these numbers.

I mentioned that as part of the outreach they are publishing these graphs, you can now go to route-trust-anchor-reports.research.icann.org and you'll see a graph that's updated weekly that shows pretty much all the stuff that I've been showing here.

This might be interesting; this actually shows the sources, the autonomous system numbers and the description of those autonomous system numbers, and you can sort of map an autonomous system number into an internet service provider, so this shows the top 30 sources. Reliance is a very large ISP in India, DTag, Telecom, AG in Germany. MobilyAS is the largest mobile carrier in Saudi Arabia, so these are source IP addresses occurring that are announcing the 8145-data indicating that the resolver is misconfigured.

ALAN GREENBERG: David, we have an absolutely hard stop on the hour, and I'd like to allow some questions, so if you can hit the high points?

DAVID CONRAD:	Okay. So, community assistance, we actually went to the ISPCP and said, "Could you help us track down the operators for these addresses?" And, went to the RRIR's and after they got over the shock of seeing 267,000 addresses, they agreed to start helping us try to track down these.
	Next steps; we're continuing to investigate data 145, trying to understand the weirdness's that we're seeing there. We're working to contact the various autonomous system number administrators. We're encouraging others to help us try to track this stuff down, and we're going to continue to publicize route KSK roll as much as we can.
	One of the challenges we're having right now is we approach various conferences to say we want to talk about the KSK rollover, and they decline the talks because it's boring; we've heard this 100 times before, we don't need to hear it again. And, we want to keep listening to the community. How you can help; again, please provide input to the public comment process, and join the KSK rollover mailing list, it's pretty low-volume, but there have been some interesting discussions there in the past. And, that's all I've got.

ALAN GREEBERG: Thank you David. I'll not to this group that we do have someone who volunteered to write our comment; he's from the technical community, you can imagine what his answer was, so we're going to have to think about it from the non-technical community.

I will say, I had a brilliant idea; I said maybe we can get users to run some sort of check to see if their resolver is compliant, and the answer from David is, "No, no way to do that." So, we can't prod them from the other end either. I have one question and then one comment; of the 100 you did contact, did they fix the problem, did they install the new trust anchor?

DAVID CONRAD: So, the 100 that we did contact, a good percentage indicated that those were dynamic IP addresses that knew where their customer's IP addresses, and they had no way to contact their customer to tell them that they were about to have a bad day. And 25% were forwarders that their customers were sending queries on behalf of somebody else, so of the others, there were folks that actually did fix, and that actual concrete fixes that we heard were people saying, "Oh yeah, I forgot to update the configuration in my virtual machine," so if they hadn't changed it, nothing bad would have happened, they would have lost resolution until they fixed the configuration.

ALAN GREENBERG: If I can summarize the statistics, I think you showed us, you said of those who have installed relatively new software, either because of a fix or just they do that kind of thing, a third of them do not have the second trust anchor installed. That implies the people who haven't installed the new software, the vast majority of us people who don't change anything until it's broken, chances are that a much larger percentage have not installed the new trust anchor, because they don't do anything to their system; in many cases they're probably software that consultant installed ten years ago, and even if you could contact the people, they'd say, "Resolver? DNS?"

So, that's the question we're going to have. We have two people who have put their hands up; quick questions, we do have a hard stop, Holly and then Hadia and John, whatever order you put your cards up.

HOLLY RAICHE: I'm going to plead complete ignorance here, but when you say dynamic allocation, which is increasing because in fact we've run out of V4 addresses, people aren't taking up V6, and is that part of the problem? I mean, you're saying you went to WHOIS,

and there was a lot of data that you couldn't get, so is that part of that problem?

DAVID CONRAD: Yeah, the dynamic addresses, if they actually are dynamic, we're not too worried about them because a resolver is usually, when it affects other users, it's usually provided via your ISP, when you boot up your computer, it'll go out and it's basically an address that can't change because it's configured into the end user machines, so if it's dynamic that means that an end user machine has requested an address, it's assigned that address, and the resolver is using that address, so it's likely it's only impacting one user.

So, in those cases the end user might go, "Huh, why is this not working?" And then figure it out pretty quickly. It sort of implies that it's an end user that actually knows what they're doing, so we're not too worried about those.

ALAN GREENBERG: David, couldn't that also be however resolver that's behind a NAT box, that it's not a dynamic address from the user's perspective, it only looks like a dynamic address to you?

DAVID CONRAD: Right, that is another concern, and one of the challenges that we have, that we can't tell if a dynamic address is dynamic. We have been talking with some large network providers who do do CGN; Carrier Grade Net, and trying to help them hunt down, but these are two or three levels of indirection, and it doesn't seem like a winnable solution there.

ALAN GREENBERG: John or Hadia, whoever was first.

HADIA EL MINIAWI: Hadia El Miniawi for the record. I would like to go back to slide number 16 please? So, it's 15. Yeah, I wanted to ask about this difference between the total and the 1159, so I don't really understand this part?

DAVID CONRAD: So that difference, the 1159, that suggests that what had happened is that they had started with only the KSK 2010, the 2010 key, and then as we were watching them, right, because we've been watching them over time, they then added the KSK 2017, so that's a good thing, it indicates that they became aware that they were not up to date, and then they added it.

HADIA EL MINIAWI: Okay, so it happened during the process itself?

DAVID CONRAD: Yes, exactly.

HADIA EL MINIAWI: Thank you.

ALAN GREENBERG: But I note, that's a third of one percent.

DAVID CONRAD: Yeah, it's a little lower than we would like.

ALAN GREEBERG: John?

JOHN LAPRISE: John Laprise for the record. Thank you for coming and speaking with us, David. As a comment, I'd say I'm hard pressed to think of a scarier presentation that I've heard this ICANN. From an end user perspective, the fact that we have an unbounded number of end users who may find themselves cut off is simply unacceptable, and I know in speaking with the GAC, or not the

ICANN 61
COMMUNITY FORUM
SAN JUAN
10–15 March 2018

GAC but SSAC, that the board has been advised on two separate occasions, in two SAC advices, I think it's 063 and 073, of actions to take, and the board has then advised ICANN org. to go ahead and implement those. As a following action I would like to know what actions we're actually taken by ICANN org. in support of those actions?

ALAN GREENBERG: Cut off in three minutes.

DAVID CONRAD: Alright, so those two resolutions were basically telling org., really, we mean it, you need to roll the key. And, as a result of those resolutions, we then initiated this process, and this process is multi-year, because we can only sort of touch things every quarter, and we're trying to do it in a very regimented fashion to minimize the chances that bad things will happen.

So, that's—63, 73, sort of triggered the forward motion, moving forward on doing the KSK roll, and then we hit the sort of head scratch moment where we decided that we didn't have enough information. We're anticipating another resolution that says, "Yes, really, we mean it, go ahead." And, that's what we'll do.

ALAN GREENBERG: We have two minutes for questions and answers, and we have Olivier and Shem.

OLIVIER CAPIN-LABLOND: Start with me, okay. Olivier Capin-Leblond speaking. Several comments and a question—

ALAN GREENBERG: I'm not going to go like this.

DAVID CONRAD: In 45 seconds.

OLIVIER CAPIN-LABLOND: So, several questions; have you considered using GEO IP databases to locate the actual owners of IP addresses or also looking at the money trail because obviously someone is paying for that IP address. I gather it probably is with the RIR's. I'll continue with the other questions and you can put them all at the same time.

Secondly, isn't it an easy way when the rollover takes place, and your system doesn't work because you've got the old KSK to just turn DNS SEC off, and thirdly, why October the 11th, because that's a Thursday, in Asia it actually turns into a Friday, that's

not the best time to go for mission critical stuff, so perhaps thing of a Monday or Tuesday for this, then you have the rest of the week?

DAVID CONRAD: So, going in reverse order because I've always forgotten the first question; the selection of the October 11th was trying to identify the least bad day and taking into account all sorts of holidays and operational considerations. The particular choice is something that was done by my team, and I don't know exactly why a Thursday was chosen other than because it fit within those constraints.

With regards to the second question; GEO IP, that was the first question, GEO IP will help us identify the countries or the specific regions, but it doesn't actually give us sufficient information to track down the actual operator of the resolver that's causing the problems. Money trail, we don't see that; the only thing we see the, and a single IP address at the route server, we then contact the operator, the operator in theory could see a money trail but there are a lot of open resolvers out there that have no money trail at all.

OLIVIER CAPIN-LABLOND: Turn of DNS SEC?

ICANN
COMMUNITY FORUM
61
SAN JUAN
10–15 March 2018

DAVID CONRAD: Yes, so turning of DNS SEC is the solution to the validation failing because of the KSK, and hopefully they'll turn it back on when they update the key.

ALAN GREENBERG: Okay, Shem was in line, he has taken down his card. If I can summarize; the decision that has to be made is; whether we do the rollover or not, the indications are that if we defer it another year, things won't' have changed significantly. If we decide to never do a rollover, if we ever have an emergency, we are really in trouble, and that's where we sit, and if we encourage people to turn off DNS SEC, they'll probably never turn it on again.

DAVID CONRAD: There is that risk; we have noticed that the percentage of people who are actually doing DNS SEC validation is falling now, some attribute that to the fact that we did not roll the KSK, so that's another bit of information.

ALAN GREENBERG: Thank you. We have a nice interesting discussion ahead of us, which we don't have any time allocated in this meeting to do,

but somehow, we'll find a bit of time. Thank you very much, David.

DAVID CONRAD: Thank you very much.

ALAN GREENBERG: Would someone from staff like to tell us what we're doing right now?

HEIDI GRUBER: Hi everyone, this is Heidi, just to let you know that right now, we have the NARALO 11th year anniversary starting out on the terrace, just directly over, if you go out the doors, you'll just see the terrace directly to the left, it is starting, so please make your way.

ALAN GREENBERG: Thank you.

[END OF TRANSCRIPTION]

ICANN 61
COMMUNITY FORUM
SAN JUAN
10–15 March 2018