BARCELONA – Joint Meeting: RSSAC and OCTO
Tuesday, October 23, 2018 – 13:30 to 15:00 CEST
ICANN63 | Barcelona, Spain

BRAD VERD: All right. Welcome. Thank you all for coming. This is the joint RSSAC-OCTO meeting. We have a number of things to took about on the agenda. So, a number of questions were sent back and forth that we will cover. Response to RSSAC questions – do we have the questions?

DAVID CONRAD: Yeah. The questions are in there.

BRAD VERD: Or, there are more slides. Okay, great. So, here's the agenda. Response to RSSAC questions. They're questions that we provided to OCTO prior to the meeting so that they could prepare an answer for them. We'll talk about the root server strategy resolution – that'll be David – and KSK rollover observations and future planning – Matt – and then RSSAC038, which was the advice.

Questions and answers.

DAVID CONRAD: [inaudible]

BRAD VERD: Do you want this?

DAVID CONRAD: Either way, yeah.

BRAD VERD: Go ahead.

DAVID CONRAD: So, you all sent us some questions. Thank you. Here are the answers that we put together.

So, the first question was, "In OCTO's interpretation, is the scope of the resolution the root server system as a whole, or the IMRS L-Root." We should probably just pick one one day. We're not there yet.

BRAD VERD: Yes, we should.

DAVID CONRAD: But, we're not there yet.

BRAD VERD: Thank you for catching onto that.

UNIDENITFIED MALE: So, our interpretation of that resolution – I'm assuming everyone knows what resolution we're talking about – is that it actually has two components. The first component is the development of a consensus

strategy with the community that is intended to reduce the risk of attacks that, I believe is agreed, are increasing due to the things like IoT and more bad people on that net and just more generic stuff like that.

Then, the second part of that resolution was sort of a direction of the Board to ICANN staff to begin implementation of that strategy once it's been finalized.

So, during the – and this has been an ongoing discussion now for, I don't know, like going on three years. At every Board workshop, I've had to get up and explain what risk there are to the root system and how we're trying to mitigate these risks for the L-Root or IMRS. The Board eventually made a resolution: "Well, then, okay. Go ahead and do that."

So, the that of what the Board instructed was to do develop a strategy with the community, in particular with RSSAC and the root operators, that would be amenable or appreciated by all of the root server operators to actually undertake, if they so choose, within their operations themselves. Then, presumably that strategy would be something that ICANN org would look at to implement on the L-Root.

So, we'll talk a bit more about this later on the second agenda item because that's sort of a strawman proposal on how to move forward on that resolution.

BRAD VERD: Okay. So, a lot of words there, but let me try to boil it down and make sure I get it. First and foremost, I think, to answer the question, it seems

like scope of the resolution was the root server system as whole. Correct?

DAVID CONRAD: Well, it's actually both. It's the root server system to come up with a consensus strategy, and then for L to actually implement that strategy.

BRAD VERD: Okay. All right. Anybody have questions? Thoughts?

Russ?

RUSS MUNDY: So, has there been any ideas or plans or discussions for how to do this joint development of ideas and concepts between OCTO and RSSAC? And, is it also appropriate to consider some of SSAC inclusion in looking at this also?

DAVID CONRAD: That's the second agenda item. We'll get to that.

BRAD VERD: Duane, you were about to ask a question.

DUANE WESSELS: Well, just to point out, in the last bullet there says, "Implement the strategy or not," so, I guess, who's … I'm confused because you said the resolution was directing IMRS to implement it, or –

DAVID CONRAD: So, I believe the resolution says to develop an implementation plan. Part of the development of the implementation plan is for us to establish the feasibility of the implementation.

So, the idea, sort of at a high level, is to work with the community to come up with a strategy. Once that strategy has been finalized, we'll then look at implementing that strategy. We will then decide during that implementation phase whether it makes sense for L to actually do the implementation.

UNIDENTIFIED MALE: Makes sense.

BRAD VERD: Okay. I have a number of questions, but I'm going to wait until we get through them all, because I think maybe you might address some of my questions in future bullets.

Anything from anybody in the room here regarding Question 1 here?

No. Okay. I think people want to ask questions, but they don't. So, I don't understand. So, we don't need to ask.

UNIDENTIFIED MALE: I'm with Brad. I just hate to ask a question that Dave can say, "Oh, in two slides, we answer that."

DAVID CONRAD: So, this is … [inaudible] mic. This is all of this slide. So, the second agenda item is actually talking about a strawman proposal to move forward with the coming up with the strategy. So, if it's related to coming with the strategy, we might put it off until that point. Otherwise, go ahead and ask.

BRAD VERD: Okay. Let's move forward, and then I think there might be questions regarding any number of things. But, go ahead.

DAVID CONRAD: Question 2 was making the observation that's there's a conflict between doing hyperlocal and the increased need to do monitoring.

The response to that question is, essentially, that we're making the observation that the use of the root as a vantage point for DNS behavior is going to be decreasingly effective over time because of additional technologies that are being deployed. Like NSEC aggressive use, QNAME minimization, TTL stretching, cache pre-fetching – all that sort of stuff.

So, we have to be able to deal with the fact that using the roots as a monitoring point is going to just become less effective over time. So, that in and of itself is not a reason to, I guess, discourage the deployment of hyperlocal, even if we had the ability to do so. And, I don't think we actually have the ability to do so. So, that's that.

BRAD VERD: I don't think anyone was trying to intend or imply – so, it certainly wasn't that we shouldn't monitor. I don't think what you're trying to say, but that's kind of what I just heard. With the deployment of hyperlocal, this effort, which you used here, monitoring every query is not going to be possible anymore. I don't think anybody was implying that.

But, I know the SSAC recommendation, the RRSAC recommendation, and the CR was all about monitoring the root server system and the health of it. So, how does that come together?

DAVID CONRAD: Come together? So, I guess what we're saying is that we are not going to be able to rely on the root as a – we're going to be less able to rely on the root as a vantage point moving forward, simply as a fact of the evolution of the DNS protocols and how people are deploying the DNS.

BRAD VERD: But – I'm going to put words in your mouth her because I hope this is the answer – you're not saying that we shouldn't monitor the root server system.

DAVID CONRAD: Right. We definitely should not not monitor … we should monitor the DNS as a system and the root server system as system. The problem is that chances that we're going to be able to continue to rely on doing

PCAPS at the roots is going to become decreasingly useful over time as more and more queries get diverted down by the resolvers, either because of hyperlocal or because of the other things that are coming along that are focused on performance or privacy.

BRAD VERD: Right, because we're spreading wider, right?

DAVID CONRAD: Right.

BRAD VERD: So, it becomes harder because it's not a captive audience anymore as far as the audience running it. It's now running it as kind of all over the place.

So, that begs the question of, what time or what effort or what is being spent on trying to figure out how to monitor it with those types of changes implemented?

DAVID CONRAD: Right. So, one of the –

BRAD VERD: Because, operationally – background – we need to know the health of the system.

DAVID CONRAD: Sure. I agree. So, one of the potential mitigations is to try to establish – and this is part of the strategy, I believe – better relationships with resolver operators, in hopes of gaining additional information that the resolvers have the best vantage point on getting some sort of aggregated data feeds out of the resolvers to compensate for the data that we're losing at the root.

BRAD VERD: Russ was first. Then, we'll go to Daniel.

RUSS MUNDY: David, one of the things that RSSAC and many others have struggled with over time – and RSSAC has talked about some this meeting – I just what does it mean to monitor the root server system as a system?

Do you view this tasking and resolution from the Board to include perhaps helping RSSAC work through the development of what that means and what and how do we lay out what the requirements and then go forward with implementing whatever that set of requirements are so that we can measure it as a system?

DAVID CONRAD: Well, I don't … I'm not sure it's incorporated within the resolution. It is something that OCTO was extremely interested in pursuing. In fact, I have a couple people on my staff who that's all they think about: monitoring the root.

So, it's something that we would be overjoyed to engage with RSSAC and SSAC and anybody else on how to improve the monitoring of the system as a whole, and in particular, the system as it impacts ICANN.

DANIEL MIGAULT: When you say "having better relations with the resolvers," do you also include the one using hyperloop? Or …

DAVID CONRAD: Hyperlocal?

DANIEL MIGAULT: Yeah.

DAVID CONRAD: Hyperloop. Not the train thing, yeah. Yeah, definitely. So, one of the implications of hyperlocal is that we would need a distribution system, and enhanced root zone availability distribution system.

One potential approach – this is sort of a pre-baked idea (or quarter-baked may be a better way of describing it) – is that, if we have a system that you can sign up for voluntarily that would send out notifies – any time the root zone gets updated, you get a notify if you sign up the service – that would actually provide us a way of contacting the resolver operators who are making use of the hyperlocal stuff. That's something to explore. It's obviously not mandatory. It'd be a way of opting in.

But, I think one of our lessons from the KSK rollover is that we have to have better relationship with resolver operators. One of the big challenges we had was just getting ahold of these people, not to identify in particular (EIR), and get them to make sure their trust anchor was updated correctly.

If we establish a relationship, then maybe we can, as part of that relationship, work out some sort of deal where we're able to gain access to their data.

WES HARDAKER: So, David, maybe you're not aware, but I actually run a project called Local Root at ISI, which allows you to do exactly what you just said. You can sign up. You get notifies –

DAVID CONRAD: I might have gotten that idea from someplace.

WES HARDAKER: Yeah. So, in fact, I'll be giving an update about it tomorrow at the DNSSSEC Workshop as well because there's a bunch of new features and stuff, and I planned for the future as well.

DAVID CONRAD: Oh, cool. I love that plan. And, to be clear, I'm not saying that ICANN should be running this. It's just, if we're going to be down the hyperlocal

path, that seems like an obvious thing that we could. If we could establish a relationship with resolvers that way, even better.

WES HARDAKER: And, I am now collecting e-mail addresses so I can contact people when events like what it just happened occur and things like that.

BRAD VERD: Any other questions?

So, I was just going to use hyperlocal as an example. Obviously, RSSAC has stated in our documents that the root operators serve the IANA root. We shared our guiding principles in the RSSAC037, one of which the IETF is the steward of the protocol. 7706 has come through that steward.

But, there are efforts that have happened from OCTO working with the software vendors that would enable this hyperlocal type of stuff.

Is that happening in conjunction with the community? If not, how do we kind of get abreast of what's going on before? Or, is it just an after-notification type of thing?

Where does this … I'm trying to think of the right choice of words here … piece of things is … are we failing as a technology group? Or, is it coming from maybe the TEG and we aren't aware of it? If that's the case, we need to figure out the conversation happens so that people are up to speed and know what's going on.

DAVID CONRAD: So, OCTO in its original inception, although it seems to be mutating a bit, was focused primarily on research on future-looking kinds of things, and SSR as well. But, an implication of that is that we try to look ahead at where things are going and to facilitate the ones that we think are relevant to ICANN's mission.

In the context of hyperlocal, as well as others – things like NSEC aggressive use and other things, like QNAME minimization – some of the direction was either explicit or implicit from the Board, saying, "Here is a risk. OCTO needs to look at how to address that risk and should facilitate the addressing of those risks moving forward."

As things have been evolving, it probably makes sense to have a wider vetting of some of the ideas, of some of the observations, of either the community or the Board in terms of the priorities that we take on in larger-scale research efforts.

In this particular case, we received explicit direction from the Board that we need to develop a strategy. Part of that strategy, in our sort of initial stab at it, includes hyperlocal. But, the Board explicitly said that we needed to work with the community to vet that strategy and finalize it. So, that is a way that information can be more easily propagated, I suppose.

The observation I'd make is that at least part of the intent of these meetings is to share what we're doing and where we are in those things. So, I would suggest making use of these sorts of venues as a way of

sharing information – we'll get to the stuff we're working on in response to, I guess, Question 5 or something like that – about the stuff that we're working on in the remainder of fiscal year '19.

BRAD VERD: Any questions?

No? All right. Go ahead, David.

DAVID CONRAD: There's a pretty picture there on the right. It's just white on white.

BRAD VERD: I like it.

DAVID CONRAD: Yeah, I like it.

UNIDENTIFIED MALE: Is it possible that it's animation?

DAVID CONRAD: No, it's not animation. It's just –

UNIDENTIFIED FEMALE: [inaudible]

DAVID CONRAD: Yes. It is a normal Internet graph, up and to the right.

So, the question is, what research informed the ICANN Board that the long-term outlook for the traditional approach appeared bleak ?

The graph that is obviously on the right there shows the increase in DDoS capacity with what looks really close to an exponential curve going upwards. So, the traditional approach of dealing with attacks has been to throw money at the problem – increase bandwidth, increase number of instances.

Unfortunately, as I'm sure all of you can attest, throwing bandwidth and throwing instances at the problem cost money, and it's costing increasing amounts of money. When you're looking at a 1.7 terabit kind of attack, that suggests a non-insignificant amount money in order to address that particular problem.

So, we didn't have any explicit research in terms of that statement, but I will not that it says, "appears bleak." … there we are. Yes. That's the graph that I was talking about … that's gone now … there we are. So, that's where we got that.

Any questions?

UNIDENTIFIED MALE: So, are the attacks on the root system?

DAVID CONRAD: No. This is just attack capacity.

UNIDENTIFIED MALE: Okay.

DAVID CONRAD: We're very clear in saying that we don't see an immediate risk to the root server system as a whole, although individual instances might have bad days.

What we're seeing is an increased risk of the threat of attack. So, over time, particularly with IoT and the nightmare that it is, we don't anticipate that graph flattening out in the near future.

GEOFF HUSTON: Thanks. A lot of this surmising and the appearance of "bleak" sort of assumes it's business as usual around the technology of how we do the DNS. I suppose the exploratory question – and it's on everyone's mind at the moment – is, if we started to look hard at TLS between recursives and authoritatives, how would that alter your picture of being able to dispose of large amounts of traffic that, at this point, because of UDP, you have no way of knowing?

And, to what extent does that kind of technology evolution offer us a small degree of possibility of being able to ameliorate this massive onslaught of "There's much more attack capacity than defense capacity, and that's just going to get worse"?

DAVID CONRAD: So, it's an interesting question because sort of an underlying requirement, or an implication, of that question is a very significant deviation from the current model of operation for the root server operators, specifically that they would stop listening to UDP, essentially.

I have some skepticism that that will occur in my – or, the ability to move away from UDP-based queries – career or my lifetime, whichever comes first.

[WARREN KUMARI]: Yeah. Your question kind of assumes that that's the specific type of attack and not a bunch of bots or doing TLS connections and making DNS queries. The type of attack could quite easily shift from bunch of packets to bunch of thingies making connections.

DAVID CONRAD: Yeah. On that point, TLS being much more expensive than UDP, you need less capacity to take out – and it's much harder to try to filter that sort of crap out than just saying, "I'm not going to listen to NTP packets that are coming at my root server." Then, you get into volumetric-type attacks that, as we've seen, can be very effective.

So, ultimately, I think there's an architectural issue here. I think the model of the DNS inherent with – is having a centralized response architecture I think might have actually been maybe not the best idea

and that a decentralized might make more sense, which goes back to the hyperlocal model.

WES HARDAKER: So, I'd like to bring some attention to my colleagues: John Heidemann's work, if you know him, who's also one of the operators at USC. He did a paper in the last six months – it was just published at IMC, I believe – where he studied the effect of TTLs against attacks like this.

So, the important takeaway is that, if you have longer TTLs, you are less subject to an outage during an attack. He studied it in a number of ways. It's actually a fascinating paper. But, one of the reasons the Dyn attack actually was so effective was that all of those companies were using five-minute TTLs. So, you only had to keep up that volume of attack for five minutes.

So, the other important thing that we need to look at is what is the length of capacity that some of the attacks are able to stay up and not get filtered at the source or other places? Because the root zone TTLs are a two-days-plus. It's much less subject to actually being taken out so easily well. Besides just the volume, you also have to consider the duration.

BRAD VERD: I have a – was there another question? I feel like I need to ask, to be a balanced question – obviously, we are DNS people here, so if I have a hammer, everything is a nail. So, trying to address this attack problem,

we're always trying to address it from the DNS side, and I understand that.

Is OCTO looking at trying to influence it on the other side, on the IoT side, trying to fix the problem versus trying to defend the problem? Is there any effort happening on that front? Obviously, that wouldn't happen here at RSSAC, but that's the balance to the question.

DAVID CONRAD: Sure. Yeah. So, there has been some discussion, yeah, even at the Board level, on that exact question. We, a while ago, had begun a project to actually look at CPE implementations of DNS clients and servers and attempt to identify the ones that were incredibly broken and then potentially go out to the vendors to get that fixed.

That project was essentially terminated, simply because of other pressing requirements and the lack of sort of entre into the various CPE vendor environments. Those, unfortunately, tend to be somewhat hard to find because each CPE does it slightly differently, and sometimes the outsource libraries – you don't even know where they come from.

So, it's something that we did look at the past. It is something that the Board has discussed on a couple of occasions. It is something that we would like to get into again. I think CERA is doing some work in sort of certification of IoT-related devices. I know the European Union is also looking at similar things to try to set a bar that would allow folks to have some certification that their DNS servers aren't stupid.

Unfortunately, the reality is that all of those efforts are going to take quite a bit of time. In many cases, the IoT devices don't do DNS, other than as clients, and they're doing DNS clients in normal ways. It's other security aspects that are abysmal that result in us not – it's not really within our bailiwick because it's more of a global infrastructure issue, as opposed to an issue that's within ICANN's remit.

[inaudible]?

UNIDENTIFIED MALE: Thank you very much, David. I think that's something we also need to discuss within RSSAC: what we would like OCTO to do on this. But, my personal position is that I'm not fully supportive of that direction – for example, addressing this source; in this case, IoT – because, if you use that chain of logic, then the second question is, where should we stop? Because right now we say the remit of ICANN is DNS [at max], if you really interpret it widely. And, if we say, "Okay. But, IoT is affecting DNS, so we have to work or try to fix issue in IoT," but tomorrow the issue might be that there are states who are attacking DNS, then do we expect ICANN to fight with the states, for example, or whatever?

So, there are many other things. I really prefer ICANN, again, personally, so we have to discuss this within our sector: to stay within the technical scope of ICANN.

BRAD VERD: Just for clarification, that was not me asking OCTO to go do anything. That was me asking if OCTO was doing anything. Just to be clear.

UNIDENTIFIED MALE: Thank you.

RUSS MUNDY: I didn't hear you mention it, David, but there is some work going on in SSAC on developing advice for Internet of Things' activities. So, you might take a look at that work party. Cristian Hesselman is the one that's leading it.

I haven't had time to pay attention to it, but they're trying to describe architectural kinds of things that are pointed at topics of this nature. So, it would be good for somebody to look at it. I'll try, but it'd help if you did, too.

DAVID CONRAD: So, can OCTO be more specific on what new technological advances and methodologies are envisioned in enhancing root server operator practices that are not occurring organically and would require ICANN org to shepherd?

So, we didn't mean to suggest that we were shepherding. It's more requiring ICANN org to shepherd. For hyperlocal, which has appeared organically, some community members have suggested that it may appropriate for ICANN org to organize or coordinate or support reliable zone availability service, but that's not to say that we would be the only place to do that.

In keeping with our mandate to ensure the security and stability of the DNS, ICANN facilitates deployment of other technologies that are developed within the IETF.

Other places to address the threats to security and stability, as we interpret them, and the stuff that we reported, has been stuff like the DNS privacy enhancements, QNAME minimization, the aggressive use stuff, and hyperlocal as well.

Questions? Comments? Screams of outrage? Flaming briquettes?

No? Moving on, so, Question 5: What are the priorities for OCTO in the coming year?

I interpreted that to be the remainder of FY '19.

BRAD VERD: Yes. Apologies.

DAVID CONRAD: Yeah. So, the implementation plan for RSSAC037/038 is high on that list. Studies on DNS abuse from using the DAAR platform – so, the SSR Review Team, Version 1, requires us to develop an SSR framework document. That needs to be updated. John and Carlos are actually working on that. We need to get that done by FY '19. It's actually late.

We want to improve our engagement with the operational security communities – folks like law enforcement and anti-abuse groups. As a

result of the resolution, we need to produce a plan to implement the root server strategy.

We're continuing to work on ITHI. We're actually going to be migrating the data into the open data platform. Speaking of which, the open data platform is being moved to production, which means that ICANN operations is going to take over the data asset inventory, and the engineering and IT group will be taking over the operation of the platform itself.

We have these root zone maintenance studies that were mandated by the transition agreement. We need to kick off the evolutionary study. We'll be issuing an RFP for that.

We're undertaking a study of resolver behavior, or actually sort of continuing a study of resolver behavior. It might be good to finish of the KSK roll. We have two more steps in the process, the next being in January. That would probably be good to do, since it's still within the fiscal year.

We're enhancing our capacity building, doing more trainings and capacity building, all over the world. We're coordinating with the Board Technical Committee. IDL is taking over that role and is going to work with the new Chair of the BTC, Akinori.

And, we publish internally some narratives, two-pages, short descriptions, on various things. We want to begin to do more public publications of technical content, more white papers, more stuff, sort

of taking the stuff we do internally and propagating out to the world to increase the ways people can yell at us.

So, those are the things that we're planning on doing for this fiscal year. It is a lot, but it's always a lot. There's probably stuff that I'm forgetting as well.

Yes, Wes?

WES HARDAKER: Two really quick questions. One might be impossible, and that's okay. So, in terms of prioritization, you said that those are not in order. Are you able to pick, say, the top three out of all those?

DAVID CONRAD: Easily. The RSSAC037/038, KSK roll, and DNS [especially] using DAAR.

WES HARDAKER: Okay. And, I did notice that the one item that I see is missing is the discussion about the next KSK roll. Are you planning on starting that sort of discussion is 2019 or not?

DAVID CONRAD: Yeah. I actually consider that part of finishing the KSK rollover. And, it's also on the agenda.

BRAD VERD: A couple clarifications. One is one the – did I just lose it? – the produce-a-plan to implement. So, that's not necessarily to implement. That's just to come up with the strategy is, as you said earlier, based upon the conversations with the community – what you're doing – as directed by the Board.

DAVID CONRAD: Exactly.

BRAD VERD: Okay. Second piece: We have a work party right now on resolver behavior. It seems like we maybe should work together on this.

DAVID CONRAD: That's absolutely tied into that. That's Paul Hoffman's work on that. That's what that means.

BRAD VERD: Great. I just wanted to make sure that we're not duplicating efforts or running in parallel.

UNIDENTIFIED MALE: Paul is the work party lead for that. So, yeah, we're talking.

BRAD VERD: Great.

DAVID CONRAD: Okay. Moving on, Question 6: Can OCTO share any internal organizational changes regarding ownership and operation of both the IANA and IMRS?

So, with Akram's departure, Goran has temporarily assigned IANA to OCTO. So, I am now the executive owner of the IANA function. That's why you heard screaming of outrage from California, regardless of where you are in the world. And, there's still much gnashing of teeth, right, [Nayla]? It's unclear –

BRAD VERD: Why …

DAVID CONRAD: I'm kidding. It's a joke.

BRAD VERD: Okay. Sorry. I was clearly missing something because I didn't understand the California joke.

UNIDENTIFIED MALE: The best jokes are the ones you explain.

DAVID CONRAD: Yeah. My impression is that the folks in IANA were not completely offended at the idea that I'd be in charge of IANA again.

BRAD VERD: I was going to say, "Again?"

DAVID CONRAD: Again, yeah. It's unclear whether that's going to be a permanent assignment. A lot probably depends on who is bringing brought in to replace Goran – Goran? I didn't say that. Akram. That wasn't me. Nope. Matt, you shouldn't have said that.

BRAD VERD: I was going to say, IANA is not like the kid that keeps coming home, right?

DAVID CONRAD: Yeah, no. it also may depend on potential restricting. Internally, we just don't know at this stage. It's only been, what, a week?

The other IMRS – Goran officially transferred the ownership of the strategy of how we deal with ICANN's root server to OCTO, but not the operations. The operations will continue to be done by ICANN's DNS engineering group – Terry and his band of favorites that you all know and love.

So, the way we've dealt with that internally is we have sort of a pseudo-contract, and SLA, that we're developing that says, "Terry's group will do this by then," kind of thing. It's sort of an internal thing that we do sometimes when we have cross-departmental type functions, which the IMRS has become.

So, I believe Goran's idea was that OCTO has more of a focus on strategic growth and future directions, which has made sense for that sort of stuff to be dumped into OCTO, whereas IT and engineering are the folks who do operational stuff, so it made sense for the actual operation of the L-Root to be done within Terry's group.

So, that's sort of the short answer.

BRAD VERD: Any questions for David?

I actually had one on the previous slide. Apologies. I forgot.

The RZM – so, obviously, as the liaison from RSAC to RZERC – but this was under discussion and was pulled. What is the plan for this study going forward, if you can share?

DAVID CONRAD: Sure. So, the plan is that we're going to do an RFP and get some expert group or something. We'll throw them money. They'll come back with a set of recommendations. Then, the recommendations are the things that we would then provide back to the Board and the Board would then provide to RZERC for their input.

Where we and OCTO sort of screwed up is we sort of tried to throw it to RZERC, which A) we're not supposed to do, because the specification for RZERC said that it was the Board or a community, not staff, but it probably doesn't make a lot of sense for RZERC to brought in this early in the game because we're not actually proposing any changes. So,

instead, when the changes are developed, then it'll get thrown over to RZERC as, "Here's some potential evolutionary changes. What does the [August] RZERC body think is the right way of dealing with those?"

BRAD VERD: Thank you.

DAVID CONRAD: Sure.

Okay. Any other questions on any of this? If not, we move on to this second agenda item. That's the root server strategy resolution. So, I'm assuming that everybody has read the resolution. Going into this, this is sort of the first draft of a plan. This is purely a strawman. It's not intended to be definitive in any way.

But, to couch it, I'm making two assumptions here. One is that ICANN is a root server operator and, as a root server operator, we can make suggestions on strategy through RSSAC, just like any other root server operator. Assumption two, it is impossible for ICANN org by itself to increase the security of the root server we operate to be able to deal with the growth of attacks to the system as a whole.

That is the reason that we actually need a strategy across the entire system. If ICANN could do it by ourselves, then we probably would. But, we can't, so we're trying to develop a strategy that all of the root server operators could buy into to allow us as a system to address the increased risk of attack.

So, those are two assumptions that I made, and one can argue them. One could also watch the screen [flit] out … okay.

Questions or comments about that?

BRAD VERD: Yeah. Maybe you're going to go through it and maybe I'm jumping ahead, but it looks like maybe some of it – the plan to come up with that strategy, you say, obviously, is community engagement. You're going to go through what that engagement looks like and kind of a timeline, or …

DAVID CONRAD: Well, no, because, like I said, this is sort of a strawman. I wanted to get sort of the broad strokes agreed upon among this community before I went sort of further on it.

So, basically, those six steps are sort of the generic plan. So, we'll come up with sort of a draft. We have sort of the beginnings of a draft that was used with the rationale for the resolution itself. But, it talks about stuff that isn't – it gives a lot of background and stuff that most people here don't care about. So, we need to clean that up and provide that as a draft strategy with full intent that it can be hacked and shredded as people see fit.

After some period of time, which is undetermined at this point, because I have no idea how long that would take, we revised that paper with input received from RSSAC and the root operators. Once there's sort of

agreement within the RSSAC, RSSAC Caucus, root operators community, we then put it out to the larger community for public comment and then, obviously, revise the paper, based on the input from that comment.

At that point, we finalize the strategy. Once we have the finalized strategy, then we would develop the implementation plan for that strategy, along with the resource requirements that we would then submit back to the Board and meet the requirements of the resolution for the Board to do as the Board please.

BRAD VERD: Any questions? Russ?

RUSS MUNDY: So, now is probably the time for my question – would RRSAC involvement at some point before it hits sort of the publication part? – be appropriate. It seems to me that it would, but I'm not certain.

DAVID CONRAD: Yeah. I would think so. It's not like this stuff would be confidential or anything. So, it'd be nice if the liaisons could share and propagate comments back and forth. Or, we could approach both SSAC and RSSAC at the same time. However, whatever is easiest is probably the right answer there.

BRAD VERD: Well, I would go so far to say that you probably need RZERC if you're talking about some extended distribution system that you touched on at least two or three times that I heard of.

DAVID CONRAD: Yeah. It's an interesting question. I don't know. I guess my impression of RZERC was , when there is concrete evolution being proposed – so, if RSSAC and SSAC and OCTO come up with a strategy that then proposes a set of changes, then routing it through RZERC might make sense. Or, do you think it would make sense for RZERC to be involved in the development of the strategy?

BRAD VERD: I don't know. I think my answer would be probably same as your answers right now. I'd need to cogitate on that, think, and figure it out. But, that piece belongs to RZERC, so …

DAVID CONRAD: Right. Yeah. Yes, Russ?

RUSS MUNDY: A consideration for making a decision would be, if even the strategy itself involved a part of the provisioning aspects, then, almost surely, RZERC would need relatively early engagement. Otherwise, probably not.

DAVID CONRAD: Yeah. I think my understanding of the intent of the strategy is to focus specifically on the availability of the root service. But, that may obviously have impact on the provisioning system as well.

WES HARDAKER: So, a couple of things. One, at ISI, we actually have a two-year research project to develop new defensive techniques for DNS servers. We are one year into it. We already produced some tools that we'll be releasing shortly, and some new filtering mechanisms – I'll draw those to your attention – that you might want to include in your … In the next year, we should be wrapping up and have a number of novel things that are going to come out of that that have proven useful.

Can you give me an idea of sort of the scope of what you envision? It may be too early, and that's a fine answer, but there's two different scopes that I'm sort of curious about. One is, what sort of solutions are on the table? To go to the extreme, we could replace DNS – just get rid of it and start using something else. That would be one – I doubt you're going –

DAVID CONRAD: That would be extreme, yes.

WES HARDAKER: That would be extreme, so that's where I'm sort of wondering: where you're falling in that gambit. Some of it also comes from, what scopes

are you looking for solutions for? Are you most looking at near-term, or you're also looking at longer-term? "How do we fix things over the scope of a decade that's going to require extensive changes and pushouts to new resolution software and things like that?"

DAVID CONRAD: So, I guess I don't really have firm answers right now. My feeling is that the scope is probably limited to what is reasonably implementable given the existing technologies. It's not something like replacing the DNS, while, perhaps, everyone would love that idea. It's unlikely to be something that's feasible, given the reality of the world.

In terms of … I forgot the second part of your question.

WES HARDAKER: The second part was in terms of near-term versus long-term in terms of –

DAVID CONRAD: Oh yeah. So, I think we've been couching it in both terms. So, there are near-term activities that can be undertaken by root server operators, just following the normal course of operations. Like, in L's case, it's just deploying more single instances in various places, or increasing the capacity into the clusters. Every operator has probably their own approaches in which to deal with these situations.

I think a strategy that talks about both would probably be the most beneficial to the Board because what they're aiming to do – the objective here – is asking staff to come up with a strategy that would

allow for them not to worry about showing up in congressional testimony, explaining why the root went down.

So, that means that it takes both the near-term and the long-term into account, because you can take the root down in the near term and the long term. So, having a strategy that addresses both of those is probably what the Board is mostly interested in.

WES HARDAKER: I agree. I think that's the right answer. So, good. I will [inaudible] comment, of course, which I'm sure you've thought. But, just to make sure, don't forget about the slow flattening of the root zone as we possibly go into a new era of new gTLDs and taking that into account with respect to the strategy and the defensives needed.

DAVID CONRAD: Yeah. That actually reminded me of something that needed to be in priority list, which was an early warning system that was identified as one of the SSAC requirements. I believe that we need to do something about that this fiscal year. So, that's another thing that I just forgot to list. Sorry.

UNIDENTIFIED MALE: More of a logistical question because we have, in a few hours, a conversation with the Board, and one of our question is very similar to this, almost – the answer, I guess – and the Board will pass, I guess, to David.

So, do we want to go through that again and then start a discussion with the Board, or do you want to remove that question? Just because, if you're satisfied with the answer, I just want to know what RSSAC prefers to do.

So, we have a question in our session with the Board –

[BRAD VERD] What is the question?

UNIDENTIFIED MALE: We submitted four questions.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: Yes, to the Board. And –

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: The root server strategy, and this answers that question. I know in the Board session, because I'm chairing that, that it will be passed to David. So, David, I guess –

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: Yes, exactly. I assume he's going to present the same slide to the same group of people, plus the Board, who has seen this slide.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: Okay.

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED MALE: Yeah. No, so then maybe we can go through quicker than it, but then there's discussion with the Board on different aspects of this.

WES HARDAKER: I'd phrase it as we had this discussion an hour ago, but if the Board members wanted to add anything to the discussion, now is the time.

UNIDENTIFIED MALE: Thank you.

DAVID CONRAD: Okay. Anything else on this? This was the last question that you had submitted to us, I believe.

Then – yes?

UNIDENTIFIED MALE: Just when you mentioned the KSK rollover, do we intend to move to elliptic curves?

DAVID CONRAD: We're going to do that tomorrow?

UNIDENTIFIED MALE: Tomorrow?

DAVID CONRAD: Tomorrow, yeah. More seriously, doing an algorithm roll is something that we will need to think about. It's something that I personally would like to do, but I don't think the infrastructure is quite there yet. Geoff might have a better idea of it; in particular, EdDSA support. And, migrating the root probably needs to be the tailing edge of the deployment of support for that kind of technology. Just my guess.

UNIDENTIFIED MALE: There are communities in South Africa, Kyrgyzstan … I've forgotten. There's a third one that is still running such an ancient version of the

OpenSSL libraries that ECDSA P-256 isn't supported. Everywhere else on the planet, if we see DNSSEC, we see ECDSA P-256. So, in some ways, it's about as close as you're ever going to get. If you beat up some up folk in those three countries – the two I've mentioned, and the other one I've forgotten – where probably …

DAVID CONRAD: How about EdDSA?

UNIDENTIFIED MALE: Oh, god, you're asking another question, are you?

DAVID CONRAD: Yeah. I've gotten the impression that, if we went to ECDSA, it would be bad.

UNIDENTIFIED MALE: So, is this a serious question? Because I'm happy to go and look.

DAVID CONRAD: Actually, I'd be interested, yeah. I'm suspecting it's going to suck, but I'd be interested.

UNIDENTIFIED MALE: Let's find out. Okay. Thank you.

BRAD VERD: If I may, the other piece of that that I hope we're looking at are the tools used to validate those things. So, that always becomes a challenge as you try to implement it in our validation steps.

RUSS MUNDY: Perhaps I missed it, but what timeframe should we be looking for something more than the slide description of the plan? Is it a week, a month, a quarter, a year?

DAVID CONRAD: Yes.

RUSS MUNDY: Okay.

DAVID CONRAD: So, I'm going on vacation at the end of this meeting, I'm not going to touch a computer for two weeks. I'll get back to you when I get back.

UNIDENTIFIED MALE: Two weeks?

DAVID CONRAD: I'll get back to Russ in two weeks to say when we'll have more detail on the plan.

Okay. So, we have two things left. There's the KSK rollover observations and future planning, and RSSAC038. Which one would you like to do first, because –

BRAD VERD: I feel like the KSK stuff would go kind of quickly, wouldn't it?

DAVID CONRAD: Yeah. It'd only take about an hour. Yeah, I have to introduce the concept and … yeah. I'll hand it over to Matt.

MATT LARSON: So –

BRAD VERD: I'm not saying it's not an important one. I'd think it'd go quickly.

MATT LARSON: Could I get a show of hands of everyone here who's heard me talk about the KSK roll at this meeting already?

Oh, fewer than I thought. All right. So, that's just if I go fast or extremely fast. So, we did the KSK rollover. That's this slide. It happened on time, as planned.

Here's the dramatic sequence of events. It took us three hours. We carefully did a lot more than we usually do when we publish a root zone

file, so everybody was extra happy with the quality of the file, that it was right.

So, here's a shot of all of us. We did it from Amsterdam because we all wanted to do it. We also wanted to go to DNS-OARC and didn't want to be a plane in that first 48 hours after the KSK roll. That young guy in the lower left, that is from 2010, when we signed the root zone. There was insistence that we do a dramatic reenactment of that picture. So, on the right, that's the whatever.

All right. So, one thing we've observed here is the number of DNSKEY queries that has the root has gone up. I apologize that that's essentially illegible. Also, I apologize that the physical size of the graphs stays the same but the scale changes.

So, the point is that there are more DNSKEY queries. This is right before the role. The role happens at the very right. Look at the upper left graph. That's the one to look at. That's all the root servers. Upper left graph.

The KSK roll happens at the far right of all those graphs. So, I think that tops off at about 1,400 queries per second at the top of the y axis – shoot, I simply don't remember and can't see what that one … but that's a higher –

UNIDENTIFIED MALE: It's like 3,000.

MATT LARSON: Yeah. Okay. Can you see that from here?

UNIDENTIFIED MALE: Sure.

UNIDENTIFIED MALE: 2,500.

WES HARDAKER: Wow.

UNIDENTIFIED MALE: Not that many.

MATT LARSON: And, the yellow line is a week ago from then. So, you can see that has increased. At the far right of the upper left graph is the 48-hour mark after the KSK roll.

Then – oh. Can you do next slide, please? Then, this is today. So, it's even a little higher today.

So, we're actively looking into this. The really short answer based on the preliminary research is that it is a very small number of resolvers sending a lot more queries.

Here's the 8145 data. Can you scroll a little bit to that right, please?

UNIDENTIFIED MALE: Or zoom out.

MATT LARSON: Or zoom out – no, you don't need to be zoomed in anymore. So, there's this odd – this is the gift that keeps on giving, this data set – little bump there. The black is the percentage of ostensibly non-ready recursives. You can see that there's this little bump in non-readiness and then back again. I forget where October 11th exactly is on that graph.

UNIDENTIFIED MALE: It's right to the left, near the peak.

WES HARDAKER: It's right before that bump.

MATT LARSON: Yeah. So, again, the more we see this data, the more I really wonder what it's telling us.

Oh, and I can't click.

UNIDENTIFIED MALE: Next slide.

MATT LARSON: Short story? Nothing happened. There were a couple of outages that are suspicious, the one at Eyre in Ireland, but nobody is talking, and I'm still trying to track down, timing-wise, the Vermont ISP. I've reached out to people. I haven't heard back from them.

UNIDENTIFIED MALE: Next slide.

MATT LARSON: Next slide, please.

UNIDENTIFIED MALE: [inaudible]

MATT LARSON: Yeah. So, here are the upcoming milestones. We've got the Q4 ceremonies, where we actually generate the signatures that will revoke KSK 2010. That happens on January 11th. So, we will have a new maximum size of the DNSKEY response from the root servers then because we'll get more RR sig in the response because the revocation has to be self-signed. So, there will be another signature from not only KSK 2017 but KSK 2010 will make a command performance one more time to revoke itself.

Then, in March, when we actually stop publishing KSK 2010 altogether – we don't actually remove KSK 2010 from the HSMs until Q3 and Q4. I don't have a slide on next steps in terms of addressing timing for the next roll and algorithm roll and whatever. I guess the high points are that the community definitely needs to be involved. It's certainly not something ICANN can do unilaterally, nor do we want to.

I do think that ICANN org is going to have to take a leadership position to the extent that, I think, without a strawman proposal to get the discussion going, I don't think anything is going to happen.

So, I see us initiating and, to a certain extent, leading the discussion but certainly not steering the discussion, but just getting it going. I would think by Kobe, for sure –

UNIDENTIFIED MALE: Sorry, Matt. Can you clarify? Are you talking about just a plan for the next roll or for something we're –

MATT LARSON: [inaudible] roll.

UNIDENTIFIED MALE: Okay. You're not talking about algorithm role. You're just talking about the next …

MATT LARSON: No. They're all together in my head as futures, but clearly, I think it's … well, we have to hear what people say. I would think we don't want to entangle an algorithm with the next KSK roll, but there might be people who think otherwise. I think we need to have that discussion.

UNIDENTIFIED MALE: Okay. I agree. I was just wondering if you were thinking that you needed all this planning for the next normal roll.

MATT LARSON: No. I think there's sort of three things that we need to sort of think of in terms of the future. One is the frequency of the normal roll, the staying with the same algorithm. Then, there's the algorithm roll itself, and then there's the third, which is, do we want to review how we do this to begin with? Do we want to look at doing a standby key? Those sorts of discussions.

So, I think it's probably best to treat those as three independent discussions, not try to merge them into a single discussion.

[WARREN KUMARI]: This is, I guess, a comment, not a question. I think I've done it a number of times already, but I'd like to say, again, that I think this went off really, really well, and also that it went off way better than I was expecting. I was predicting there'd be a bunch of outage. People kept telling me that I was wrong, and it turns out I was wrong. Well done. Thanks for doing this, and sorry for the drama before.

MATT LARSON: I expected a whole lot of outage, too, so …

DAVID CONRAD: Okay. So, moving into the last agenda item that we had, it is a discussion on RSSAC037/038. For this, I have asked the staff person who is actually going to be do the work to actually come in and talk to it. So, Karen?

KAREN LENTZ: Thank you, David. For those who I haven't had a chance to meet yet, my name is Karen Lentz. I was recruited a few weeks ago to work with OCTO on this project. So, I've immersed myself in RSSAC037, and the discussions this week have been helpful to me in getting up to speed on this work and this project.

The slide that you're looking at is the three recommendations from RSSAC038, the [advice] which is the actual advice to the Board, which I think you're familiar with.

But, first of all, that the Board initiative a process to produce a final version of the model. Secondly, that we do some cost estimating of the root server system and on developing the model. Thirdly, that we, having completed both of the other steps, work through that process and implement a final version of the model. So, those of the three pieces of advice that the Board has right now under consideration.

Can we go to the next slide? So, in terms of the planning and status of the work, we're following a process which we've been using recently to track and consider the advice that the Board receives from advisory committees. That includes, first of all, confirmation that there's a

common understanding of what the advice is, which I believe exchange on that has occurred already.

But, secondly, there's the drafting a document called the feasibility assessment and implementation plan, which is essentially a road map, as we're calling it here. But, that's a document that's presented to the Board to help determine the next steps. So, that includes visibility, assessment of things like resources that it will take to develop the model, timeline, steps, etc., and the implementation piece, which is the process by which we get to a final model.

So, I have the task of drafting that document. As David has mentioned elsewhere, I think our timeline to be able to deliver that to the Board is the end of the calendar year.

But, to go back a little bit to the process question of what's the right way to take this model forward – the draft initial model that RSSAC has presented – in a timely and efficient and way and also make sure that we have an opportunity for all of the affected stakeholders to be able to have input and review into that process, it would be helpful at this stage to hear any guidance that RSSAC might have on the process itself as we're working to draft the options for how we might approach that. But, if there's a vision of how the process should occur or what you'd like to see or not like to see, that would be helpful input at this point.

BRAD VERD: Thank you. I think the response to your question of – any input that we'd – I guess, as the Board, as ICANN org, consider 037/038 and go

forward, we, RSSAC, are willing and, let's say, want to help. If I tried to compare it to something, this is a large body of work coming out of an AC, which is a little out of the ordinary, let's say. We just went through our organizational review, and we just did our feasibility plan for the review.

We had a work party inside RSSAC that worked on that plan back and forth, worked with the independent reviewer, worked with [MSSI]. There was a back and forth over this stuff through the whole process, and, if that type of process could be used here, I think it would be more than welcome because, then, when we get to that end, that final implementation plan, everybody is on the same page – we can hit the ground running type of thing – versus something else being derailed because things went off in a box for six or so months and came out and it was the first time we see it type of thing.

So, if we could do something like that – RSSAC has talked. I think we would love to help with that.

KAREN LENTZ: Great. Thank you.

DAVID CONRAD: Yeah. And, I think, doing the work together, obviously, makes the most sense because it'll hopefully be able to allow us to have direct access to the concepts behind the words because a lot of clarification is frequently necessarily. Having direct access, I think, will improve our ability to be able to respond.

BRAD VERD: Really quickly, Russ, I agree with that. I think the group is eager to share, eager to work with you guys because, as you said, there's a lot of thought and discussions that went on that maybe aren't in the document that, as you work through the plan, we would like to help with.

RUSS MUNDY: I'd like to speak up in strong support of what I just heard and draw a parallel to a different set of activities that had some similar characteristics. That was the planning for the KSK rollover that was done, for the most part, but OCTO. The plans were good, were thought through, and the whole activity – but it was conducted in this isolated set of sort of the big spectrum of a small part of the world.

In the end, when the Board made the decision that they wanted to get, as some members have described to me, a second opinion and they came to the SOs and ACs with an incredibly short timeline and not a well-formed question, it was a very painful exercise for a number of people. I think, if we can do all we can to avoid something similar, it will produce a much better answer for the community and a much better set of outputs for everybody.

BRAD VERD: Just to build on everything – I keep saying that – we know this is kind of an exception. It's an exception for us. Normally we give advice and – I don't want to say walk away, but it's kind of cut and dry. This is

different. So, I think it would be beneficial for all parties involved if we stayed involved.

UNIDENTIFIED MALE: Yup. Agreed. And, I think that's all we got.

BRAD VERD: Any questions for us from OCTO?

UNIDENTIFIED MALE: We just spent a few minutes saying how great it would be to each have input into the process. How do we do that?

DAVID CONRAD: Yeah. As Brad said, we'll probably need to figure that out. But, I'd imagine that, as a minimum, we'd have regular briefings at these sorts of meetings, where we provide you with information. We'll probably be setting up a joint mailing list or something like that, where we bounce ideas back and forth. But, it's something we need to explore to find out the best mechanisms to allow for the information propagation.

BRAD VERD: Well, obviously, the next meeting is after your timeline for providing something to the Board. Then, I assume, the Board would look at it in Kobe. So, I'd we'd look at it or at least know what's going on prior to Kobe, and then, I assume, the Board will cogitate on it and spend some time with it after they get it in Kobe, or a little bit before, for their

workshop. But, intended to say the same thing to the Board later today, which is, "We would like to be involved in this process so that the product is what everybody expects and wants."

DAVID CONRAD: Yup. Agreed.

BRAD VERD: We'll hear from OCTO via mail, I guess, as to what happens next on this.

DAVID CONRAD: Yeah. Probably from Karen or myself. Karen has quite a bit of experience in these sorts of governance implementation-related issues, so she's been down this road a couple of times and survived it. So, I'm going to be relying on her quite a bit.

RUSS MUNDY: As the SSAC liaison to the group here, I wanted to let the group know that, yesterday, when we had our joint meeting, I pushed forward the point that SSAC should make comments on RSSAC037, even without any explicit Board tasking. Whether or not SSAC will want to say anything prior to getting Board tasking is unknown, but I wanted to be fully open and above board. I'm trying to get SSAC to think about it right now, and, if they have something to say right now, to say it.

UNIDENTIFIED MALE: I think, at a minimum, we could invite Karen and the OCTO team to the monthly teleconferences. We can work with the Co-Chairs to schedule that.

BRAD VERD: Anything else anybody wants to – I'm sorry. I think you had a question. No? Anything else anybody wants to bring up while we're all together.

John Crain is in the room. I did not see that until just now. Welcome, John.

JOHN CRAIN: Thank you. It's very strange I'm no longer on RSSAC.

BRAD VERD: All right. If nothing else, we will adjourn. Thank you all.

DAVID CONRAD: Thank you.

[END OF TRANSCRIPTION]