SAN JUAN – Joint Meeting: ICANN Board and RSSAC
Thursday, March 15, 2018 – 10:30 to 11:30 AST
ICANN61 | San Juan, Puerto Rico

KAVEH RANJBAR: We are going to start in two minutes.

David, I think it's good if you have -- if you can please sit at the table, please. Thank you very much.

Okay. Let's start the meeting. Jonne, please, the main table.

So let's start the meeting.

Is there anyone from RSSAC or the Board who is not sitting at the main table? Because we have seats. If you're not, please join us at the main table.

Good morning, everyone.

Welcome to the public session between the ICANN board and RSSAC. Let me kick off this meeting first by going through a quick roll call, and then we will go through our agenda.

Should I start with George? George, could you please introduce yourself.

GEORGE SADOWSKY: George Sadowsky.

DAVID CONRAD: David Conrad, ICANN CTO.

AVRI DORIA: Avri Doria, ICANN board.

RYAN STEPHENSON: Ryan Stephenson, RSSAC, DOD.

JONNE SOININEN: The Jonne Soininen, IETF liaison to the ICANN board.

LITO IBARRA: Lito Ibarra, ICANN board.

KAVEH RANJBAR: Kaveh Ranjbar, RSSAC liaison to the ICANN board.

BRAD VERD: Brad Verd, Co-chair RSSAC.

TRIPTI SINHA: Tripti Sinha, co-chair RSSAC.

CHERINE CHALABY: Cherine Chalaby, ICANN board.

CHRIS DISSPAIN: Chris Disspain, ICANN board.

BECKY BURR: Becky Burr, ICANN board.

RAM MOHAN: Ram Mohan, SSAC liaison to the ICANN board.

JEFF OSBORN: Jeff Osborn, member of RSSAC.

DANIEL MIGAULT: Daniel Migault, IETF liaison to RSSAC.

GORAN MARBY: Goran Marby, ICANN org.

KAVEH RANJBAR: Thank you very much.

RUSS MUNDY: And Russ Mundy, SSAC liaison to the RSSAC. Out of breath, sorry.

KAVEH RANJBAR: Welcome, Russ.

BRAD VERD: And there are a number of apologies from the RSSAC members who are not here. A lot of them have already jumped flights on their way to London for IETF. So just want to extend their apologies.

KAVEH RANJBAR: Thank you, Brad.

Before first starting and going through the questions, I want to set the tone for the meeting. This is in informal -- this is a board meeting with the RSSAC. But we prefer to keep the tone informal and have a dialogue between the Board members and RSSAC members. We already have a set of questions. We will go through them. I just want to emphasize we want them to set the tone and the framework. But we really want to have dialogue. It's -- opinions said here might be of individuals, individual RSSAC members. That should be stated. Also from the Board. It's not going to lead to any decisions. Decisions, as usual, will

be made based on formal advice which is given from RSSAC to the Board. I think this is a very good opportunity to use this hour to clarify if there are any questions or any comments that board members have in their mind to use this time to clarify it.

With that, can we go to the next slide, please.

These are the questions from ICANN board to RSSAC. Basically, there were two questions. We'll start with the first one.

What are RSSAC's key goals in 2018? For that I'll leave it to the chairs.

TRIPTI SINHA: Thank you, Kaveh. And thank you for the questions.

In terms of our key goals for 2018, there are three. And I'll start with the very first one.

As some of you are aware, we've been working for roughly three years, close to three years now on some key advice to the Board regarding the next phase or the evolution of the root server system. This was put in place many decades ago. And the model has been roughly more or less static and hasn't evolved in any way.

So we've spent a fair amount of time digging deeper into this model and addressing some questions that have been

outstanding for many, many years now such as the accountability measures built into the system. Who are we accountable to? Who are the stakeholders? How is this funded? How is it sustained? How will it continue to grow and scale to the ever-growing Internet?

So we're very close to wrapping the advice up. In terms of our timeline, we have a draft version. We intend to have a version -- a very close to complete version in May at the RSSAC workshop.

Our intent then is to socialize that version with the Board at your workshop and have this voted and finalized in June.

So, currently, barring any unforeseen problems and delays, we will release the advice in -- at ICANN 62. So that is primarily our focus at this time.

The second focus that we have is, as you know, we were recently reviewed. And that is currently underway. That will likely complete in April. And we will have recommendations following that review. And we will work through those recommendations with the relevant committees.

And we also have the RSSAC caucus which focuses on numerous and sundry technical issues. And we have roughly three works under way in that area.

So that is our current three areas, key goals for calendar 2018.

CHERINE CHALABY: I have a question.

TRIPTI SINHA: Sure.

CHERINE CHALABY: Sorry, Tripti. The advice, the timing, you're going to release it at ICANN 62. Yes? Did you say you want to socialize it with the Board beforehand?

TRIPTI SINHA: Yes. The plan is to socialize this with you at your Vancouver retreat, if we can get on the agenda.

CHERINE CHALABY: Excellent. You will get on the agenda. Yes, that's good.

KAVEH RANJBAR: We already requested a time slot.

CHERINE CHALABY: Absolutely. I remember. I apologize. On the SSAC review -- RSSAC review, sorry. Any comments on the effectiveness on the review so far? What's your reaction?

TRIPTI SINHA: So our understanding was this was an organizational review. And it was to look at RSSAC, the advisory committee and the dynamics of the committee and its continuing purpose within the ICANN ecosystem.

And we felt that it quite didn't hit that mark. It wasn't an organizational review of RSSAC, and there was some -- I might speak to the confusion that exists currently within the community on what RSSAC is and its role and the other community members that make the RSSAC, define the RSSAC, which are the RSOs, root server operators. But our sense was that it was not an organizational review, per se.

CHERINE CHALABY: And the reason I'm asking that is that we are hearing a lot from different parts of the community and constituency about the effectiveness of the reviews. And there seems to be some common theme that we ought to, first of all, look at the amount of reviews done in any particular year and try maybe to stagger those and do each one more effectively rather than do quite a lot all in one year and compress -- so, for example, next year there are nine reviews planned. Right?

And would the RSSAC be in support of also kind of almost everybody else saying the same thing, look at those holistically and say, you know, can -- do we have the volunteers to do all of this? Do we have the resources to do all of those in one year? And should we stagger those over maybe a two- or three-year period and do less but do better?

TRIPTI SINHA: Completely agree with you. In fact, we would like to provide some input. And we do believe that you need to take a step back, look at the process holistically. And also the effectiveness of the reviews. What is the intent and what is your desired outcome? I think you need to provide more guard rails in how these reviews are conducted. Ensure that they are kept within scope, define the scope very strictly. And the tone of the report -- the reports need to be instructive and constructive in value.

CHERINE CHALABY: Okay. So, Goran -- sorry, on the reviews, your plan is to send the consultation paper out after -- what's the plan? How to collect more input?

GORAN MARBY: Thank you, Cherine. This is Goran.

There are sort of two different things here to talk about. One of them is the bylaws mandated reviews. The cadence of that.

And when to start, when to stop them. So that's sort of one discussion.

And that's the ones I'm intending to -- with the support of the community, send out some sort of information. Because it's -- if we're going to do something, that is a bylaws change itself.

And the other thing you're raising -- I think that is also a very important question, which has been raised not only by you but also what are the intents of the reviews?

What is the -- what do you want out of them? What is the effectiveness?

And I know that in the OEC, these discussions are started to come up as well.

I don't have a plan for that, that part yet. And I shouldn't, because this has come from the OEC within the Board. And this will be a dialogue within the community. But it has been raised several times to me this week. Because we spend a lot of -- sorry. We invest a lot of money and time in the reviews itself. And some reviews have been going on organizationally -- some reviews have been going on for a very long time. I think at-large has been doing it for four years. And that's another discussion.

So, on that particular point, Cherine, I have to formulate that and go back through the OEC, have a dialogue with the Board. And funny enough, there is the chairman. So he can now continue. Thank you.

KAVEH RANJBAR: I have Brad and then Khaled.

BRAD VERD: I was just going to say the RSSAC is preparing two responses. One response to the independent examiner in the hopes of -- to share our feedback on the assessment in the hopes that, if the recommendations that have yet to come out are, as Tripti said, instructive and constructive. And then the second feedback we're preparing our thoughts on the entire process that will be shared with the OEC.

KAVEH RANJBAR: Khaled, please.

KHALED KOUBAA: Thank you. just to share with you that indeed the OEC has had an informal discussion this morning, 7:30. All the members are here as well. And we have acknowledged the increase of feedback that we are receiving from the community in regards

to the reviews. We acknowledge as well the unsatisfaction of a lot of constituencies about the reviews, their process, their way of how we are doing them. So there will be for sure different actions. As Goran said, there will be short-term action, mid-term action, and long-term actions.

We will not be able as OEC to make any discussion as for now because we need to finish this meeting, digest all the comments and feedback that we are receiving from the community, and then let ICANN org work on the structuring all those feedbacks in a very evidence-based and informed decision which will allow the OEC to present to the Board the recommendations.

So we will be very active on that because we have seen the sensitivity of this issue and how much it's important for the community to really tackle the reviews in a better way. And, again, I mean, for the long term, it's also to ask the question what is the impact? What impact those reviews are having on our organization? And -- but this is also a long-term issue. Thank you.

KAVEH RANJBAR: Thank you very much, Khaled.

Any other questions? Cherine, please.

CHERINE CHALABY: Not on the reviews. If there's a moment, I'd like to talk about the advice on the evolution of the root service system.

KAVEH RANJBAR: Please.

CHERINE CHALABY: Now?

KAVEH RANJBAR: Yes.

CHERINE CHALABY: Okay. So the issue that is in my mind is about cost.

I don't know if you will be in a position to provide indication of costs to implement your advice or it's something that we can work together with. Because what's happening at the moment -- and you've seen it across almost all the -- all the stakeholder groups that -- so this morning, for example, we met with the SSAC.

And they're saying the amount of work that's coming their way for them to provide advice, they can't -- they can't deal with. There's a cost issue. There's a resources issue.

And we, the Board, just take the reverse. Advice that come our way, they all have a cost implication to implement.

So in that particular one, because this is a critical one, would you be able to give an indication of costs? Or is something that we need to work together on it?

TRIPTI SINHA: So I think there are two questions regarding costs in it. One is the cost of just putting the advice together by the -- in our case, the advisory committee. And I must say I was taken aback by just the sheer amount of work and time and commitment that has gone into this the last three years.

And there has no cost been associated with just that amount of work. Now, when we deliver the advice, there's clearly -- if this is to be implemented, there's going to be a cost to the implementation itself. Just the implementation. Then there's another cost which is the cost of the model. Once we have an operational model in place, to operate this new infrastructure and service. Yeah, that's the new -- whatever the root server system model is. That, of course, will be a hefty cost upon the stakeholders and so forth. So we're really and truly talking about three different costs.

Now, are we going to include any numbers in our advice? Not in this version, that was not our intent. However, we -- the way we understand that this work will work is that we will deliver the advice, the board will ruminate on it, and you may come back with questions and ask us to do a deeper dive on, say, the financials. Do a deeper dive on so on and so forth so that you -- that we will then peel the onion away and take a look at these issues more deeply and then at some point, it's either a go or a no-go. And as I said, there's going to be implementation costs if there's a go and then the cost of the model itself.

BRAD VERD: Yeah. And I think that feedback process that Tripti just described is with both the board and the community.

CHERINE CHALABY: Okay. And one more question on that because it's important. So this affects the root server systems and by default the root server operators. Will the advice be a consensus advice with the agreement of all the root server operators or it's just an RSSAC advice without the full consensus and agreement of the operators?

TRIPTI SINHA: No, there will be consensus certainly of RSSAC, and we have been very explicit in saying that it is incumbent upon each of the RSOs that are contained within the RSSAC to feed this information back to their parent companies so that before we sign off on this they are aware that the RSOs are signing off on this and they support this model. So yes, this will -- there will certainly be consensus there.

When this is implemented, we believe this problem is much bigger than RSSAC and that it will be a community-driven process. Because there are many individual boxes went into this model that are outside of our skill set.

KAVEH RANJBAR: Thank you very much, Tripti. Okay. Any other comments or questions from the board or RSSAC on this? Okay. Seeing none, I just -- for the record, I want to say since the roll call we have from the ICANN board we have Maarten, Lousewies, Lito, Ron, and Sarah and Matthew in the room and Khaled. And Leon. Oh, yes. Sorry.

Okay, going to the second question, this is -- again, the board is asking RSSAC what are the most long-term relevant goals of RSSAC. And to frame this, this is basically because the board is working on the next five-year strategic plan, and the main reason for asking this question is to get a feedback from RSSAC

and our constituencies basically as an input for that strategic plan. So actually this is a very important question I ask for us. I know this will continue also in Panama, but for now, if RSSAC has any comments on that. Brad, Tripti.

BRAD VERD: Well, I think we've already touched on this. I think our most relevant longer term goals would be the implementation of the advice that we will be providing at ICANN 62. Obviously there will be, you know -- we expect a back-and-forth between the board and then a much larger effort with the community. This is the start of a conversation.

KAVEH RANJBAR: Thank you very much. And as it was in Cherine's opening remarks, I think also that this is already recorded as one of the -- one of the upcoming priorities for the board, correct, Cherine? Okay. So can I move to the next slide, please? The next slide. Yes.

So these are questions from RSSAC to the board. I will start with the first one which is the concerns of the board about root service or if -- if there are any pressures that are observed by the board to -- observed by the RSSAC toward the root servers. Ram.

RAM MOHAN: Thank you. Ram Mohan. The board's most significant concern related to the root server system is the threat of DDoS attacks that may overwhelm the entire system. The threat is not specific to the root server system, of course. Every service on the Internet is at risk. The board has been discussing what options ICANN org has to help mitigate this threat. Unfortunately, there are few actions that ICANN org can take that can have an immediate and direct effect on the threat.

The most obviously short-term mitigation appears to be adding root server capacity, but this comes as a cost and certainly there's a time limit associated with it as well. Do the root operators have an intention to expand capacity and do they have the resources, financial, personnel, et cetera, to do so. So these are some questions that have -- that the board has discussed internally. The board is also interested in seeing the overall accountability of the root operators improved.

Regarding pressure the board perceives about the root server system, the board sees non-technical driven demand for additional root operators. The board is aware of the need for ICANN org itself to take all reasonable actions to mitigate DDoS threats. And finally, the board is aware and acknowledges the community's desire for greater accountability for root operators.

So that's -- that's what has been the primary discussion inside the board.

KAVEH RANJBAR: Thank you very much. So to give a bit of background, we also, in our public situation with OCTO, we also have been presented by what was proposed by OCTO as mitigations that's coming from the ICANN org or possible solutions to mitigate some of these issues, and they were having a bit of discussion also the next steps in that threat is those -- that proposal from OCTO has been submitted formally to board technical community. Next time board technical community convenes, which I guess will be next week there will be -- over an email threat, we will discuss on how to move forward. I assume contacting RSSAC and SSAC is one part of that. And so that -- that threat will continue.

In the meantime, I think RSSAC already has shown interest in those and already -- there has been already some discussions and some opinions about some of those supporting or for some of them we have some concerns. So I would like to ask Brad to start.

BRAD VERD: Yeah, I'm going to -- I'm going to do a bunch of questions in there, so I'm going to jump around on you and I'm going to save

the DDoS one for last because I think that will be probably the richer dialogue. Regarding the accountability from both the board -- the accountability question from the board and from the community, I believe, as we've stated, we are working on that, and we believe that that will be addressed in the upcoming advice to the board. So I hate to say stay tuned, but it -- we -- we've spent a considerable amount of time on this. And we -- we -- and the idea was to go through all the pitfalls and challenges that -- that we -- that we could foresee to ensure that the model addressed all of them. So -- and that's what's taking time.

Regarding the non-technical demand, I think that is going to be not addressed specifically in the evolution work but it will give you the tools for the board to implement as they see fit to try to address that. That is a political challenge and this is a technical committee to -- you know, to advise the board. So it's -- it's a bit of a gray area there.

Capacity -- sorry, capacity for the -- the root servers, I think I can -- I can just point to the growth of the current -- current platform that serves the root. It was not long ago, I want to say a year, maybe a little bit more than a year ago, we were sitting here saying 6 -- 600 instances worldwide. Now we're somewhere north of 950 instances worldwide. So the growth is continuing and ongoing. And that is, as you pointed out, one of the first lines of defense for the -- the DDoSs -- the DDoS risk. I think

echoing what OCTO put together around L-Root and shared with both the board and RSSAC, it -- it mimics exactly what's being done by the root server operators today. So everything you see in there that calls out L specifically, you could just apply to any of the letters today. So there's -- everything's happening by all the operators.

Regarding DDoS, I think, again, the threats have been there. This is not a new threat to the root server system. This is an existing threat that -- that the -- that RSSAC has been concerned with. The root server operators are concerned with. As you can tell by the expansion and the money being invested by each of the operators to expand the platform. I think, as you stated, this is a non-specific threat. Anybody who's on the Internet is at risk. I think in our discussion with OCTO earlier this week there was an interesting question or kind of point made which was wow, the root is at risk, like any other platform. The -- there are probably some TLDs that are -- have the same risk and could have great impact in a shorter amount of time. And so there were -- there was lots of discussion around that, so it would be something to look at.

With that, I will -- I think I've addressed all the points. So if I missed one, please let me know and I'll try to come back to it, or someone else can.

KHALED KOUBAA: Thank you, Brad. Cherine?

CHERINE CHALABY: So the question that we've put in here begs another question, why now? And let me explain it a little bit. And I may seek your help in the answer. So our mission has always been to secure and ensure the stable and secure operation of the Internet identifier system. The root server service has, for the past -- since the inception of ICANN, been very stable, right? And working. So I think we ought to -- we owe it to RSSAC to explain why now suddenly we -- we're raising this issue, right? I mean, it has been stable. It is true that our missions say we have to ensure that. We don't have direct authority over the root server operators or any of that kind to do anything else. So why now this issue is now important? Ram, you may want to just explain the changes that we see in technology that make that a pertinent question now, which was not before.

RAM MOHAN: Thank you, Cherine. The -- the discussion inside the board has been, we acknowledge and understand that the DDoS threat itself is not a new threat. But what has increased the board's attention to this is the -- the fact that we're now at terabit scale

attacks and the increase in those terabit scale attacks, the rate of growth of that appears to be far exceeding the rate of growth of any capacity increase that is happening. And again, we recognize that this is not just at the root system itself. The root server system itself.

The second piece to add to that is the concern that there is a proliferation of devices that are constantly connected to the Internet that in their native state come with vulnerabilities and allow them to be corralled into botnets, et cetera, far more easier than it used to be before. Combined with the fact that there are open source based systems that allow for these kinds of devices to be chained together into a very large network of attacking devices, that can potentially overwhelm the entire system. So it's -- it's not that DDoS itself is an unknown thing. It's that the rate of growth on the attacking side appears to be racing far ahead of the conventional methods of responses which have typically been about capacity building and adding, you know, more bandwidth, more iron to respond.

KAVEH RANJBAR: So just let me start the conversation. I see representatives from six root server operators here out of the 12 organizations. So may I ask a question directed to all of us root operators?

Do any one of us lose sleep over these threats? Because I think technically we all understand the magnitude and the possibility of these threats to the root server system. But do any one of us lose sleep over that? Or do we feel, oh, the sky is falling so we need to be -- please.

JEFF OSBORN: Jeff Osborn with ISC. We are the operator of the F-root. And one of the strengths of the root server operation is its diversity of method. And so all of us sort of are different organizations that do things differently. And the combination of them, I think, has a great strength to it.

So ISC is a stalwart in the Internet. It's been around forever. My employees have been around for mostly over a decade. The Board between the four of them have something like hundreds of years of Internet experience. It's a deep organization.

And in the last year and a half, we've literally added more than an order of magnitude of bandwidth capacity in combination first by upgrading all of our hardware that existed in the field and, second, in partnering with CloudFlare which is a provider of just huge amounts of bandwidth, pretty much around the globe. I was in Kathmandu two weeks ago when we brought up the F-root instance in Kathmandu.

And the kind of volumes of data that we're fearing now literally don't cause the pagers of a CloudFlare guy to go off. So going from working by ourselves in a place where a sustained gig attack was noticeable and people would be concerned, we've gone to a place where it's an item in a log. It's really not an issue at all.

I saw in the OCTO report, it looks like ICANN isn't choosing as a root operator to go that direction. I think that's great. I think the fact that we have a divergence of opinions on this is really excellent.

To put a really crazy pie in the sky idea out there, my board loves the idea of getting ten thousand tiny little Anycast devices and spreading them all around the world so you have catchments that are so small that a DDOS storm never has a chance to build up ahead of steam because everything is absorbed by sacrificial anodes, if you will, dispersed widely around the world.

The strength of DDOS is that a whole bunch of things all come together on one target. And the nature of Anycast is such that you get absorbed by your local instance instead.

So there is no dearth of us thinking about this. But I don't lose sleep over it. I think we are moving in an interesting direction.

And the last thing I'll say is if we get up here and brag about how attack-proof we are, we'll get our phones ringing and being told by our ops people that that just caused an attack. So by definition, we have to be a little humble, and that's an unfortunate message for you to receive.

KAVEH RANJBAR: Thank you very much.

I have Lyman, then Ram, and then David.

LARS-JOHAN LIMAN: Lars Liman from Netnod. We also operate one of the instances.

I would like to add to all of that, that there are also other defense mechanisms being deployed. And they're on the sides of filtering, on the sides of relationships between the root server operators and the various Internet service providers who are the involuntary carriers of the attacks towards, in our case, the root servers.

There's an entire network of people and organizations with the good intent of keeping things up and running. And that is -- that is actually a notable resource. So we are not on our own in this. There is an entire -- there is an entire Internet out there that wants to help us.

Thanks.

KAVEH RANJBAR: Thank you very much.

Ram.

RAM MOHAN: Thanks. I want to refer back to something that was said that, you know -- the report that OCTO put out that spoke about the expansion of the L -- L-root instance, L-clusters and L-singles, et cetera, that those kinds of expansions you could apply it to all of the other letters.

Inside the Board, there is not clarity that there is that same kind of investment or that same kind of focus on capacity planning that is happening. It doesn't mean that it isn't happening. It's that the awareness is not there.

The other concern is that we may go from, you know, 1.7-terabit-persecond-scale attacks to 5-, 7-, 10-terabit-scale attacks.

And the concern is: Will -- is there appropriate planning? Is there appropriate risk management? Are there -- what kind of mitigation mechanisms exist with those who are entrusted with operating the root server system?

So I think that level of dialogue and that kind of education of the Board I think will be extremely useful to reduce some of the concerns that exist.

Another thing that might be useful -- and this might help in the accountability piece is to have at some high level a report on the investments or the capacity expansions, et cetera. Perhaps at some uniform metalevel that can be made available to the community because it's not just the Board that's hearing this. It's also hearing from members in the community. Thank you.

KAVEH RANJBAR: David, is it in relation to that? So anyone wants to answer that directly. Yes, if you answering for that answer, please.

BRAD VERD: Couple thoughts. One, I just want to point out this is really an operational line of questioning, which is a reasonable line of questioning but I want to point out this is an operational line of questioning and RSSAC is not necessarily responsible for the RSSAC. As it's also been pointed out, there is no kind of operational accountability outside of L.

So I think -- I don't want to lose sight of the fact that the evolution work that we're working on. Our goal is to address kind of the organizational governance and the operational

accountability in that model. Now, I know that's a future thing and that's an immediate -- there's a risk that is forcing kind of these operational questions. So we understand there is -- kind of like there's an immediate need and then the future deliverable, if that makes sense. I don't want to lose sight of that.

Speaking candidly as a root operator, not as an RSSAC person, I think it is -- I don't know how I feel -- I certainly don't know how my organization would feel about a metareport showing capacity and investment because what you don't want to do, because it is critical, in infrastructure is provide a roadmap for the bad actors. So that's just something to keep in mind as we have this discussion.

You know, you don't want to publish exactly what my capacity is. You don't want to publish any number of different things. So it's just something to keep in mind at an operational level, not a policy level but as an operational level, that that is a risk that needs to take -- be taken into the account, by the Board, by the community, by the people who are asking as to how far that -- that needle moves, if that makes sense.

RAM MOHAN: Very briefly, Kaveh.

Brad, that's -- I think you'll find complete alignment on the Board with that perspective. There is a very strong awareness that there is no desire to provide a roadmap for the bad guys to figure out what to do and how to attack.

Part of the questioning or part of the thing that we have to work together on is that one of the discussions I remember very vividly from one of the Board workshops is a question of: Let's take the case where there is a significant attack and a -- you know, some part of the root goes down, who is going to be brought up in front of some committee? And what is the question that's going to be asked? And the question that's going to be asked is: Were you aware that there might be a threat? Were you aware that something -- you know, that there was a significant threat and that might take a piece of this part of what is perceived to be the core of the Internet down. What did you do about it, right?

So I think part of what we're trying to do is to collaborate and work to get to a -- both a narrative as well as real answers on that while keeping in mind that on the operational side there is no desire to expose all the things that all of you are doing. It's important work. It's good work. We don't want to expose that. But at the same time, I think there is a desire from the Board to have some visibility and some level of confidence building that

that work is happening, more than just hearing a "trust us, it's happening," right?

So I think that's -- I think that is what's going on. Sorry to be somewhat candid about it. But I think this is the nature of what is actually happening on Board discussions.

KAVEH RANJBAR: Thank you. Any answer for that? Tripti, please.

TRIPTI SINHA: So, Ram, just a two-prong answer to your question. So, one, we completely understand the Board's position, that you're going to need a narrative. And we respect that. We understand that. And threats have always existed, whether it be a nuclear threat or weapons threat or cyber threat. And it's been on our radar, and we continue to improve our operations to the extent possible. And I understand we need to give you an aggregate report of some kind to tell you this is what the root server operators are doing in aggregate. And I completely agree with what Brad is saying, is that we don't want to expose the internals of what we're doing but we can certainly put together some kind of aggregate report to reassure you it's on our radar. And it's been on our radar for decades. This is not related to just root server systems. It's just about any kind of threat.

Now, this exact reason is why we've been working on this advice because we realize we need accountability. Who are our stakeholders? We're all a dying breed. We've been here since the inception of the root server system. Some day we won't be around. We need to turn this over to somebody and create this new model, and that is what is driving us to do this. But in parallel, we are continuing to fortify the service. We do it differently. We're all 12 different organizations. There's tremendous diversity. But, you know -- I don't know if this answers your question.

KAVEH RANJBAR: So I asked for David's permission to continue this thread before getting to his comment. So if -- and we have ten more minutes to spend on this subject.

RAM MOHAN: Just very briefly. I don't think this is a question we're going to resolve here, but this is the start of a really good dialogue. And what we need -- and I'll speak personally. I'm not speaking for the Board.

Personally, what we need is some mechanism to continue this dialogue on an ongoing basis, not only at the sessions but some intersessional way to do it because, as you point out, these are --

these are threats that we are aware of and there are other threats as well, right? And I think we need some -- some mechanism to have this be a continuous loop, and we're not there yet.

But I'm personally very eager to find some way to do that because the ability to be able to sit down and say to you, Hey, we're worried not just about the operational piece but also about the fact that if, when something really happens with operations, something does happen, right, what do you say that is credible and that is also backed up by facts? You know, that's something that can only be done when we engage in a regular dialogue.

BRAD VERD: The only thing I will add -- and this is really quick. Your comment about it's 1.7 now. It's going to be 5 and 6 terabits later. I think -- you know, it was five, six years ago that we were talking about what a one-terabit attack would look like it and how we plan for it and how we try to manage around it.

So I think this is kind of the normal push and pull between the good guys and the bad actors, right? They take one step forward and then we respond. The attack vectors are always changing. So there is no, like, one silver bullet that addresses everything.

You are continually adding tools to your tool box to deal with the bad actor.

KAVEH RANJBAR: Thank you very much. Any other questions or comments regarding this? Yes, please.

RAM MOHAN: Just briefly, and I notice Lito is here as well. Lito and I co-chair the Risk Committee on the Board.

The fundamental thing that I think we're looking at is a risk management approach; right? It's not about knowing what all the solutions are, but it's understanding that the -- the risks as well as mitigations have been thought through and that then -- and some level of comfort that the mitigations have a reasonable chance of success.

KAVEH RANJBAR: Okay. If there's no other comments -- David, please.

DAVID CONRAD: Yeah, I just wanted to clarify one point. The Board report that OCTO provided to the Board and subsequently to RSSAC was intended as a set of options that the organization is considering in the context of the operation of L-root and also options related

to protecting root service. It was not intended to indicate a decision had been made about what particular approaches should be taken.

We did provide some suggestions as to what OCTO's opinion of sort of rational approaches would need to be undertaken, but some of the options that were being proposed within that document would imply a nontrivial amount of resource expenditure.

So as much as I would love to be able to dictate where expenditures would be made, that's a little above my pay grade.

KAVEH RANJBAR: Thank you very much.

So should we move to the next subject? If there's any comments or questions, I'm willing to -- okay.

So second question from RSSAC to the Board was basically about perspective of the Board on proposed KSK rollover plan. And for that I will -- basically Board defers to David to answer that question about KSK rollover.

David.

DAVID CONRAD: So the situation we're facing right now is we have data that suggest that when we do implement the KSK rollover that some percentage of the resolvers will be misconfigured and will fail resolutions if DNSSEC validation is turned on. But that data is actually not very helpful because the original KSK rollover design was focused on the users that would be impacted, and the dictates within that document suggested that no more than 0.5% of users would have a negative impact to the KSK rollover. If that were to occur, then we would back off.

So right now we're in a period of attempting to gain additional public comment on a proposed plan to move forward with the rollover on October 11th, 2018, regardless of the data that we receive related to what's known as 8145 reports from resolvers.

So I guess part of the issue is what RSSAC's view on that proposed plan would be, and what RSSAC would propose to do to mitigate any risks and concerns associated with the rollover.

KAVEH RANJBAR: So to repeat what was -- so what was also said in the meeting with the OCTO, as the timeline was shown, in May the idea is -- there's a very good chance that in May there will be a resolution from the Board asking RSSAC and SSAC to also provide advice, but that's just because of how it works. There are a few steps that should be passed before Board can issue that resolution.

So in the meantime, nothing stops SSAC or RSSAC to actually start working on advice, or if they have any comments or input for that process, to issue an advice. So please keep that in mind and schedule work if it's needed.

Thank you very much.

For the last question, it's actually basically a timing. Because the question was asked, and in the meantime there has been some advice issue that I will defer to Brad to explain.

BRAD VERD: Yes. I think this question might have been overcome by events. This -- This question was kind of in response to the GNSO question where they stated they were looking for responses from the different ACs on adding I think upwards of 25,000 names to the -- to the namespace.

And I think given the -- RSSAC has responded, SSAC has responded, and this question was created for the Board long before those transactions took -- took place.

So unless there's something more to add, I'm not sure -- from the Board perspective, but I think this question has been overcome by events.

KAVEH RANJBAR: Thank you very much, Brad.

Any other comments on that subject?

Okay. If not, is there any other topic that anyone from the Board or RSSAC wants to share or discuss?

Or, for that matter, because we still have a bit of time, anyone from the room, although mostly this is open to observers. But if there is any real comment related to RSSAC or Board relationship with RSSAC, I'm more than happy to accommodate that.

Okay. Hearing none, we are concluding this session.

Thank you very much for joining. Cheers.

[END OF TRANSCRIPTION]