DANIELLE RUTHERFORD: Thank you all for joining the RZERC monthly teleconference held on Tuesday the 19th of April 2022 at 19:00 UTC. Tim, would you like me to start the roll call?

TIM APRIL: Yes, please.

DANIELLE RUTHERFORD: All right. IETF, Tim April.

TIM APRIL: Present.

DANIELLE RUTHERFORD: ASO Carlos Martinez, we have regrets. ccNSO, Peter Koch?

PETER KOCH: Yes, present.

DANIELLE RUTHERFORD: ICANN board, Kaveh Ranjbar?

KAVEH RANJBAR: Present.

DANIELLE RUTHERFORD: PTI, Kim Davies, we have regrets. RySG, Howard Eland?

HOWARD ELAND: Yes ma'am.

DANIELLE RUTHERFORD: SSAC, Geoff Houston?

GEOFF HOUSTON: Hi.

DANIELLE RUTHERFORD: Verisign as root zone maintainer, Duane Wessels? Duane, I saw you on mute but I can't hear you. Can anyone hear Duane or is it just me?

GEOFF HOUSTON: It’s me too.

UNIDENTIFIED MALE: I don't hear him.

DANIELLE RUTHERFORD: Okay, I'll note that Duane is on the call and we might have some audio issues. My apologies, Duane. And then we have RSSAC, Daniel Migault?

DANIEL MIGAULT: Yes, that's me.

DANIELLE RUTHERFORD: All right. Tim, over to you.

TIM APRIL: Thanks, Danielle. The first item on the agenda is reviewing the minutes from the February meeting. If anyone needs to talk it over or if there are any questions? Otherwise we can take this as accepted. I don't see anything. Okay. The next item, I believe, was the ARR with Danielle.

DANIELLE RUTHERFORD: Yes. All right. This is the correct slide, Steve. So I wanted to share an update on RZERC003. Three of the recommendations have moved into phase four, which is the implementation phase, since the Board considered RZERC003 on 24 of February and took the following resolutions. So you can see that the first three bullet points show the Board accepting recommendations one, two, and four, and directing the ICANN president and CEO to implement the recommendations. In the rationale for the resolution we see that recommendation three was addressed and not included in the resolution since the recommendation was not directed at ICANN Board or Org.

The action required and next steps for these updates is none. There's nothing required, this is an informational update only. If RZERC has any comments it would like to provide to the Org at this time, I'm happy to

submit those to the advice team and on to the SMEs who will be implementing this advice.

Other than that, recommendations one, two, and four will be moved to the implementation phase and we should expect semi-regular updates as that progresses. And then recommendation three will be closed out and we will not be receiving implementation updates on that one. Does anybody have any questions about this update? Or would you like time to sort of review it and digest?

DANIEL MIGAULT: So, yeah, definitely I would like to digest it. But the immediate question I have is are there any implication of RSSAC? Anything that RSSAC is involved into? I don't see it but—

DANIELLE RUTHERFORD: No, I don't believe that there's any implications for RSSAC at this time. I think the relationship that I see is the Board directing the Org to implement already existing RSSAC advice if I'm remembering RZERC003 correctly. But no, there's no action for RSSAC at this time.

DANIEL MIGAULT: Okay, but is the Board expected to reach out to RSSAC or? I only see the root zone maintainer.

DANIELLE RUTHERFORD: Sorry, my apologies. 003 is related to ZONEMD. No, I don't believe that the Board is expected to reach out to RSSAC at this time.

DANIEL MIGAULT: Because I see the root server operators, so that's individually?

DANIELLE RUTHERFORD: That'll be up to the subject matter expert who is in charge of implementing the advice. And so that might be an implementation we see. But that'll be coming directly from ICANN Org, that won't come through the RZERC.

DANIEL MIGAULT: Okay.

DANIELLE RUTHERFORD: Does that make sense? So now that it's on the Org to implement, it'll be assigned to a subject matter expert who will design a project plan to implement recommendations one, two, and four. And that person in their capacity might reach out to root server operators. I don't know at this time if they plan on doing that individually to root server operators or through the RSSAC.

DANIEL MIGAULT: Okay.

DANIELLE RUTHERFORD: Are there any other questions at this time? Not seeing any hands, I will go ahead and acknowledge those updates on behalf of the RZERC and then they'll be removed from the action required tab on the quarterly report from the advice team.

So the next thing we have is Duane Wessels has submitted an updated ZONEMD deployment plan. And then, Duane, did you want to present this? Steve is sharing it on the screen.

DUANE WESSELS: Yeah, is my audio working now?

DANIELLE RUTHERFORD: Loud and clear.

DUANE WESSELS: Okay, good. Yeah, thanks, Danielle. So we talked about this as a couple of months ago and I've made a couple of changes to the document. The top there is just formatting and table of contents stuff. The next changes that I noticed on the root service website that we're now up to 1500 instances, so I bumped that up. Go ahead and scroll down, Steve.

Okay, and then some of these changes are really just changing sort of future tense to past tense. So, for example, in the case of the section Verisign, RZMS, and distribution system. So this work has been completed so the Verisign systems have been updated to support the record. Although that feature has been deployed, it's not yet enabled. I wanted to make sure that was clear.

And then the next section is something that we spent a lot of time talking about previously, sort of about how the roots server operators are expected to behave. And I took this issue to both the root server operator meeting and we talked about it in RSSAC as well. And in those meetings there was quite a bit of support for the deployment plan saying something along the lines that I believe, Geoff, you originally raised the issue that the plan didn't say anything about how a root server operator should behave in the face of, say, a verification failure.

So I've attempted a rewrite here in a way that places a requirement on Verisign and IANA to sort of work with the root server operators and set the expectation. So I'll just read it out for completeness. It says Verisign and ICANN are asking the root server operators to ensure their internal zone distribution systems and name servers can support the ZONEMD record. So that part has been known for a while and that communication is already underway.

The new part is and that ZONEMD verification will not be enabled for at least six months following the initial deployment. During that six-month period the RSOs must not fail to update or load the root zone due to an incorrect or missing ZONEMD record. Deployment will not begin until confirmation from all RSOs has been received. And six months is just a starting point. It's just something that felt about right to me. If people have concerns about the amount of time, that’s certainly easy to change. But really, I'm hoping that this language satisfies the concerns that were previously raised by the committee.

So I think it would be good to stop here and talk about this one, because this is really sort of the big one, I think, that's outstanding.

GEOFF HOUSTON: Duane, Geoff Houston here, I'll take down my hand at some point. What it says is for the first six months even if you can't validate, is that the correct verb?

DUANE WESSELS: Verify, yeah.

GEOFF HOUSTON: Verify. If you can't verify the ZONEMD record, you'll publish it anyway, you are merely a vehicle of conduit for the ZONEMD record. But what's not specified is after six months what is a root server operator meant to do if, A, it is doing verification of the ZONEMD record? And, B, it fails? So is it still just a conduit and it faithfully passes on what it receives from basically the zone master? Or does it go, I'm not sure I want to publish this. Therefore, I will continue with the old version of the root zone until I get a zone where the ZONEMD record validates? I mean, you've left this unstated after six months and it's not clear what a root server operator is supposed to do here.

DUANE WESSELS: So in the discussions we had with them I get the sense that some root server operators would explore enabling the verification such that if there was verification failure they would postpone, they would continue to serve the old zone, your second option in your question. I don't think all of them would do that. And I don't know what sort of timelines they're considering other than our six month ask here. But I do think

that some of them would use ZONEMD as a check in the distribution process of the root zone in their internal systems.

GEOFF HOUSTON: I am, I suppose, not entirely comfortable with the way this is sort of panning out. It disturbs me a lot that we're leaving it up to individual root server operators whether they serve a version of the zone or not depending on this single record. And the potential to have the root servers serve different SLAs and different incarnations of the zone file worries me a lot.

Now, this is after the six months. So I'm not arguing about the six months where basically these things are merely conduits. The issue is, I suppose, one interpretation of ZONEMD is that it's a second check from the root server operators to actually look at the integrity of the zone that they're being passed to serve. And if it fails that integrity test they will not serve it.

The second interpretation of the ZONEMD record is that it has nothing to do with the root server operators per se, and it's an integrity record used by folk who are pulling down local zone or some other whole of root zone and that it's the end clients who use this to actually check that the zone that they've got is the real deal.

Now, this paragraph goes to the former where we are almost stealthing in a second verification check for the root servers as root server operators, but without really exploring how we continue to serve an integral root zone if there is the unlikely event of a failure. And the only way I can conceive a failure is you're using open SSH, I'm using Geoff's

favorite SSH library and my library is different to yours and I'm going to fail the test.

Now, this is conceivable, this is not entirely outlandish and so I'm a little bit worried that after six months we're sort of going, “Not our problem.” And I think it would serve us all if we came down clearly on is this intended to serve both masters, both root server operators and eventual end clients? Or is it intended to serve only potential end clients and the whole issue about root zone integrity between the root server operators is not intentionally addressed in this document? Or is it something for both parties?

I know I'm rambling a bit. It's early in the morning, but is my question clear?

DUANE HOUSTON: Your question is clear. I do have, I guess, two points to make. I think there may be somebody else—Well, Peter put something in the chat, But I'll say my two points.

So one of the things you said was that you are uncomfortable with the idea that if there's a problem, one root server may serve one version of the zone and another one may serve a different version of the zone. But the fact is that that can already happen today, right? I mean, the zone is updated twice a day. And it's not really all that—Well I don’t want to say uncommon, but it does happen that due to network partitioning or bugs or whatever an operator may fall behind by a day or so in its version of the zone on some instances.

So this does already happen to some extent. And I think that most people are sort of okay with that because the root zone is not designed to be, you know, it's designed for sort of loose coherency. It's not intended to be updated within the order of minutes, it's okay if it sort of falls behind a little bit.

So your main question, though, was is what we're designing here, is it just for the serving root on loopback [crowd,] or is it also for the RSOs? And to me it's for both. Not initially for both, but I think eventually it's for both. And I think some root server operators welcome this additional check and would plan on using it when they're comfortable with it and when it's appropriate.

GEOFF HOUSTON: In response, and I think this is about the last thing I should say because I notice Peter has got his hand up. I think that really shouldn't be flagged as an RSSAC matter, or a root server operator, whatever. But it is really a matter that the intention coming out of this is that root server operators may use this as an additional verification check and should, capital should, design procedures to respond to verification failure in a timely manner should it occur. Because I think we're punting here on what's going to happen if you do fail and I would like at the very least to punt in a direction. Now if we punt going you guys, root server operators, RSSAC should indeed create procedures to alert, alarm, and respond if you are doing verification checks, if it fails. I think that's only responsible. Thanks.

DUANE WESSELS: All right, thanks Geoff. Peter, you've been patient, thank you.

PETER KOCH: Yeah, thanks. No worries. I was just going to support the idea that this discussion that the two of you just had and these considerations that were brought up by Geoff be added to the document, especially when it comes to what is signal and what is noise as in is it a mere transport, a mere conduit of ZONEMD? From my perspective it wouldn't make sense if the root server operator notices that ZONEMD fails verification and then still would serve the zone. That cannot lead to useful results in one way or another, except that the consideration is that there might be a failure only in the verification software, which is possible, of course. But then that's, again, the signal. Other than that it is probably not to protect the end user out there from what new systems or something in that direction.

I think that's why I wrote in the chat that this this may use ZONEMD as a signal, might be a hint. But then again, it also might be more details to be developed by RSSAC rather than RZERC.

DUANE WESSELS: Go ahead Daniel.

DANIEL MIGAULT: So far I understand that basically I should report RSSAC to clearly position itself whether the ZONEMD verification will be an additional check, yes or no. And if it failed, what is it that a new procedure should apply and should be defined?

DUANE WESSELS: Daniel, this is Duane. I don't know if we're quite to that stage yet because it feels to me like what Geoff is suggesting and what Peter is supporting, it sounds to me like that's going to end up being a new recommendation from RZERC, perhaps. It doesn't feel to me like it's part of a deployment plan because you're asking another group to do something specific.

So I guess I'd like your thoughts on whether or not this can be stuffed into this document or whether we need something new. Geoff?

GEOFF HOUSTON: You know, there's an issue of formal procedure and there's an issue that's sort of staring me at the face in this text. So the practical issue of what's staring me at the face in this text is we define that for the first six months if an RSO cannot validate the zone file, they should not do anything, that's what we're saying. And it really does beg the question, what happens after six months?

And so in practicality the issue is we should do more than this. And if the intent is, and you, I think, reiterated an intent that I support, that the ZONEMD record is a tool for root server operators as well as for end clients of the root zone, then it is incumbent on the root server operators, I believe, but it's incumbent certainly on someone to define the procedures as to what happens when such verification fails.

Logically, I think a consistent response from the root server operators would be desirable. And that's certainly clear. But who should define

that operational response? My inclination is that this is an RSSAC matter because in terms of scoping, it seems a bit odd to me that RZERC would go that deeply into this subject. But nevertheless, I'm less concerned about where that flows in terms of process, and more concerned that it should not go nowhere. It should not be as this document simply goes, full stop, after six months we're not going to say anything. I think we should say something. And I see Peter Koch's comment and I think we're saying the same thing. Thanks.

DUANE WESSELS: Okay. So I get the gist of what you're saying, that this document before you is lacking any text on after the six months period. So that's relatively easy to solve. But to your other point about somebody else developing some specific plans or operations around enabling ZONEMD, I guess my question is do we want Daniel in his liaison role to just take that to RSSAC and that's fine? Or do we want something more formal, a more formal recommendation to RSSAC?

GEOFF HOUSTON: I'm kind of beyond my organizational competence. My own instincts would be for Daniel to carry the message as a low overhead. But others might want to see a more formal message created, message passed, message act, which becomes a formal recommendation. I suppose either way works for me and I would follow the views of others if there are strong opinions either way. So I'm happy either way, but as long as something is said in this document, and whether it becomes a formal

recommendation or is simply picked up through the liaison channels, I am happy either way, personally.

DUANE WESSELS: Okay, thanks Geoff.

DANIEL MIGAULT: So I can say that I'm going to carry that to SSAC. Regarding a more formal way to interact because, I mean, we are a little bit in a chicken and, how do you say, chicken and egg issue because we have this deployment ZONEMD document that we are sort of asking something else to be provided in order to publish that one. And so, I mean, we can provide a recommendation as if we have never seen the deployment on MD document and ask it to the board and the board then and ask it to RSSAC. It might be heavy, but that's the only way I see how we can have this formal approach. But I might be wrong on that. So I mean, taking the informal approach, that's going to be done in a half an hour. And given the feedback, I might ask them whether they prefer also a more formal approach or not.

DUANE WESSELS: So I noticed that Kim has joined. And I don't want to put you on the spot, Kim, but if you're able to sort of glean from the context of what we've been talking about, and if you wanted to raise any points about this section, please do. Otherwise maybe we should move on to the other changes to the document.

KIM DAVIES: Hi, Duane. Hi all, sorry for being late. Are you referring to the root server operators section?

DUANE WESSELS: Yeah, yeah.

KIM DAVIES: So I came in midstream.

DUANE WESSELS: Well, let me catch you up a little bit. So what we've just been talking about is, so there's changes before us. These changes, they talk about a six month sort of period during which time the RSOs would not change anything, they wouldn't fail to load a zone. But after that we don't really say what they should do. And so we need some revisions here, some additions here to talk about post six months what could happen.

And then sort of at the same time we're talking about going to RSSAC to sort of, I guess, have RSSAC work on what it would look like if the RSOs want to enable ZONEMD verification. What that would actually look like and how that would work from their point of view.

KIM DAVIES: Okay, thank you. I mean, I don't really have any particular perspectives to give at this time. I think this is the first time we've made sort of a significant change under the context of RZERC, so it pays to be deliberative where we can since we don't have a per-worn path to

follow for this kind of request. Beyond that, didn't really have anything insightful to add.

DUANE WESSELS: Okay. Yeah, thanks, Kim. All right. So are folks okay if we go on to the other hopefully less controversial changes then?

GEOFF HOUSTON: I'm okay to move on, but I also would like this resolved at some point in the future.

DUANE WESSELS: Yeah, well, so would I.

GEOFF HOUSTON: I don't think we can leave it hanging.

DUANE WESSELS: I don't want to leave it hanging. I mean, I think our choices are either we can spend time now wordsmithing it or we can do it between meetings and come back. Which would you prefer?

GEOFF HOUSTON: Look, I'm happy for the wordsmithing to happen elsewhere. As I said, I'm ambivalent as to which way it does get resolved. I just would like to see it resolved. So if we would leave it like that and note that it will be wordsmithed through the meetings, that's okay by me.

DUANE WESSELS: Okay. So the next change here is in the section that talks about recursive resolvers serving root data locally. Just a little bit of clarification here because I did run some tests with Unbound, which is really the only recursive server that currently supports it. And in the case of Unbound it has to be specifically configured to perform verification, it does not happen by default. So that's really a clarification about Unbound.

All right, let's go down then. So in this section, this is where we were talking about sort of the native record format versus the generic record format. And the change here is accepted the recommendation to add a reference to the specific texts from RFC3597. And as a part of that the second part here, which is for this reason the initial invitation, that was just moved from below. It was moved up above the sample generic record format. So I think that should satisfy the concerns that were raised before about RFC3597.

Okay, so this is something that we've already really talked about before. This is, again, changing a future tense to a past tense and then reiterating something from the section we were previously talking about the RSOs, where it says that they must not enable verification until at least after six months after the initial deployment. So that's just a prerequisite for the whole process to start. There's a hand up?

GEOFF HOUSTON: Yeah, I just put my hand up because here, Duane, I actually know we've got a raised flag about root server operators should do X. And we've

done this without actually doing it as a recommendation, or as a noted liaison issue. We have just simply said they must do this. And for wordsmithing previously, I would have thought this kind of phraseology would be okay. Because that to my mind, that second sentence, is a liaison issue at the start and becomes a flag to, presumably Kim, to confirm that this is the case from the root server operators, and we're doing so without a formal recommendation.

DUANE WESSELS: Yeah, that is certainly the intention with this text. So if I understand correctly, you're saying that you like this and it's okay and it doesn't need to be changed? Is that right?

GEOFF HOUSTON: If it's good enough here, it's good enough in the previous discussion as well. This kind of root server operators must do something, I think, this is a reasonable thing to state in this context and it would be reasonable to state in the previous context about verification, yeah.

DUANE WESSELS: So in the previous context, my intention was that it was stated very similarly, maybe the words weren't exactly the same. But here it says Verisign and ICANN are asking the root server operators to ensure, so still it places the burden on the liaison's roles as you said. Would you like to see these words more matching exactly than what they are here? Is that kind of what I'm getting?

GEOFF HOUSTON: No, I would like to see the wordsmithing of the root service operators to include they must take steps after six months to ensure that validation failures are handled in a manner that results in timely, I don't know, rectification.

DUANE WESSELS: Yeah, okay. Got it. All right, thanks.

STEVE SHENG: Duane, this is Steve. Can I ask you a question?

DUANE WESSELS: Yeah.

STEVE SHENG: Has the draft been shared with the root server operators, of the plan?

DUANE WESSELS: Not this version. The previous version was shared with them.

STEVE: Okay.

DUANE WESSELS: The RZERC is the first to see this version two here.

STEVE SHENG: Okay. And my understanding is that in the original RZERC003 recommendation is the responsibility of root server operators is to verify and confirm, right?

DUANE WESSELS: Yes.

STEVE SHENG: The addition of the record will not negatively impact the distribution of the resumed data within the RS. So they are not obligated to verify it, right?

DUANE WESSELS: That's right.

STEVE SHENG: So in this deployment plan, or as it's being discussed now, are we saying that the root server operators needs to do more than what is recommended in RZERC003?

DUANE WESSELS: I think yes, in the sense that the additional request is essentially a promise that verification would not be enabled for at least the six month period. So that's sort of a new tidbit that wasn't in RZERC003.

STEVE SHENG: Okay. And what Geoff was mentioning, after six months the additional thing by root server operators, is that a big step within the six month or is it—You know, I'm just trying to understand the scale of that.

DUANE WESSELS: A big step for the root server operators, you mean?

STEVE SHENG: Yes.

DUANE WESSELS: I don't think so. I think based on the discussions that we're having now, the way I would see this moving forward is that Daniel, as RSSAC liaison, will raise this issue with RSSAC. And essentially the way I'm thinking of it is RSSAC probably needs to write a document which describes expectations of root server operators should they choose to enable ZONEMD verification. And so that might be an RSSAC publication, I'm guessing. That's sort of the default. And along with that, I would say that no root server operators should enable verification until those expectations are finalized and published. So is that kind of the question you were getting at?

STEVE SHENG: I guess my question is isn't it up to like PTI and RGM to ask the root server operators instead of RZERC? I guess that's fundamentally my question. Because this is the implementation plan and it's up to the

owners of the implementation plan to make that request, right? I'm just trying to understand. So my apologies if it's a wrong question.

DANIEL MIGAULT: I think the main concern is not that they don't do the verification. The main concern is that all the RSOs do the same thing. So if we step back to RZERC003, I mean, we're not mandating with RZERC003 data verification of [inaudible]. But I think the concern from Geoff and Peter is that there is core interactions between the RSOs.

DUANE WESSELS: Right.

GEOFF HOUSTON: I can phrase this as a scenario, I suppose. And let's say that half of the root server operators use a different cryptographic library than is being used by the root zone maintainer and everyone else. So half of them have deviated off to use canoe libraries. And there's, for some reason, a subtle structural problem inside that library that fails to validate a particular incarnation of a ZONEMD record. Now, if the root server operator is doing verification but it's not alerting and alarming, then they will get stuck on a zone version and not move indefinitely, assuming that every single time the ZONEMD comes out that they fail to verify it.

And unless there is a procedure in place to go, I've got a problem, we all need to figure out what this problem is because this is going to last indefinitely, rather than an operational problem with corruption of a

zone file in transit. This is a long-term kind of, I'm wedged. And really, it's just trying to alert to the root zone operators that they should have thought through this scenario and have some form of response that they have designed in their individual operation and in the collective operation. And it might be, well, I'm going to serve it without verification for a while until we resolve this. Or I'm going to escalate and get everyone to look at this and let's change whatever cryptography, let's change this so it gets over this problem that verification is not a consistent outcome.

I don't know, but I'm kind of saying we shouldn't just be punting this into nowhere. That's all. So I would lean, Steve, towards this is an RSSAC liaison issue, rather than a formal document item inside the PTI and RZM. But I'm not the expert here in that space, so I'll defer.

STEVE SHENG: Okay. No, I think we agree on the substance, it's just what's the right channel?

GEOFF HOUSTON: True.

DUANE WESSELS: Do you want to go to the bottom of the document again? I think we made it to the end, but I'm not 100% sure. Yeah, so that was the last change. Oh, that's right, there was this. There was a request at our previous meeting for some details on how people can contact or where they can go for questions and problems. So the proposal is to use the

Verisign customer service email address for people if they have problems about ZONEMD.

GEOFF HOUSTON: I have an appearance question on this. Sorry, I'm being a bit nit-picky this morning, I must be awake or something. So they are contacting Verisign in the role of root zone maintainer, yes?

DUANE WESSELS: Yes.

GEOFF HOUSTON: You might want to subtly say inside that sentence that users experiencing problems blah, blah, blah, may contact the root zone maintainer via Verisign customer service. Because it's not I'm ringing up Verisign because. It's I'm ringing up the root zone maintainer and their front of house is Verisign's customer service.

DUANE WESSELS: Sure, happy to do that.

GEOFF HOUSTON: Yeah, thank you.

DUANE WESSELS: Peter, you've got you hand up?

PETER KOCH: Yeah, thanks. So this invitation makes me wonder, first of all, how and where would some of these rollback decisions that were mentioned earlier in the document be communicated? And maybe more to the point, is the average resolver operator or the average hyper local operator a target audience for this deployment plan? And are we introducing a new player like the RZM to the overall system? That seems to happen to be in passing a bit to me, but maybe I'm wrong.

DANIEL MIGAULT: So, Peter, are you asking if I am running my local root, if I can connect to the RZM directly?

PETER KOCH: Yeah, that is the practical operational question. The target audience question is the umbrella question for that. So is this just an information to the community and the targets are the root zone operators or is this now for everybody? And how are we dealing with scaling in the first place? Because the other question that would have to be solved in that context probably is, how would—And we've, I think, decidedly distinguished these issues. How would a hyper local systems scale and where would people find the sources for the zone to transfer in the first place? And I'll be not giving any information about this, but the deployment plan is saying if there are any issues, please contact here. That might work, but it would probably leave another void or another gap to be filled, again, not necessarily by RZERC.

GEOFF HOUSTON: I've just pasted in the chat, I think you've opened up a large topic area, Peter. And I think it's a valid topic area to open up. And I think in terms of the role of local root, I think there is an evolutionary component that I believe is in scope, Tim might be able to do a better call. But I would not, if you will, make that larger topic a contingent on this document. I think this document can happily exist without answering the larger question of what are we going to do about local root? Which is really the question that you have raised. Thank you.

DUANE WESSELS: Yeah, I would definitely agree with that, I wouldn't want to try to tackle that harder question here in this document. To Peter, I think one of your original questions was who's the target audience for this? And I guess in my mind it's sort of at this point people who are interested in this new feature. I don't think that there's a really significant deployment of hyper local root at this point, such that, for example, it would overwhelm our customer service line or anything like that. But we did note that there was, you know, the absence of a contact point was noted previously, so this is sort of the obvious choice here, I think. But I guess I'm reluctant to say that everyone who wants to do hyper local root, please feel free to contact Verisign with your troubles, that's definitely not what I want to say.

DANIEL MIGAULT: But why having Verisign customer line as opposed to PTI or IANA, for example? I mean, if we have something wrong in the zone, who should

we contact? Let's say a TLD is missing. I realize one TLD is missing, am I not supposed to contact IANA for that?

GEOFF HOUSTON: Before we dive down this rat hole, and it's a fine hole—

DANIEL MIGAULT: That was not the intention.

GEOFF HOUSTON: It's scaled in size for many rats. I think we should indeed, if this is in scope, we should basically do it in a future meeting. Because I don't think, again, this document needs to answer that question. It's a good question, though. And someone should answer it at some point is what I'm saying. And if it's an RZERC question, yeah, let's go there. But all I wanted to do in that comment was to make sure that Verisign is being accounted for as its role in the root zone manager in this context. So it's not I'm ringing up Verisign because I just feel like ringing up someone. I'm ringing up a role and in this case, for the moment, the role is Verisign as root zone manager or whatever, RZM, and that's it. And that's all this document needs to say at this point, there is someone to contact, there is a role and a point. In the longer term, as you're pointing out, is this the right thing? Great question, don't know.

DUANE WESSELS: So, I mean, thanks for going through all the changes with me. And I've noted the feedback and we'll continue to revise, I guess, and bring it

back to the next meeting with the points that still need to be resolved. I think that's it unless there any last-minute questions on the deployment plan topic.

STEVE SHENG: What was the action item on the last point about this? So you will revise this paragraph and then after that we'll decide what to do next? Or Daniel should already taking this message back to RSSAC? I just want to get some clarity on that. Thanks.

DUANE WESSELS: Yeah, so certainly, I will need to update this paragraph with one or two sentences talking about expectations of RSOs after the six-month period. And Daniel can also take it to RSSAC. Daniel said something like 30 minutes, which I'm not sure it needs to be that urgent. But certainly, it should be something discussed at the next RSSAC meeting.

STEVE SHENG: Okay, sounds good. So then the action item is for you to update the document, in particular this paragraph. And then for Daniel to go to the RSSAC asking those questions?

DUANE WESSELS: Yeah.

STEVE SHENG: Thanks.

GEOFF HOUSTON: And the final contact sentence at the end of the document.

DUANE WESSELS: Yeah, that one was easy, I made that in my source document already. But yes.

GEOFF HOUSTON: It's almost a formalism, yeah.

TIM APRIL: Anything else for that document? Not hearing anything. Okay. Any other things to discuss on the monthly call? And I don't know if people have noticed that the charter review session was scheduled starting in six minutes or so for the next hour. Unless there any objections to just adjourning this meeting and starting that one.

DANIEL MIGAULT: So do we stay connected or?

DANIELLE RUTHERFORD: It’s separate Zoom links so you’ll need to exit this meeting and then join the new meeting.

DANIEL MIGAULT: Okay.

TIM APRIL: See you over there.

DANIELLE RUTHERFORD: Thank you everyone.

DANIEL MIGAULT: Okay, and see you there. Bye.

[END OF TRANSCRIPTION]