ANDREW MCCONACHIE: This is a meeting of the -- we don't have a work party name but it's devising the RSSAC's response to IANA's Public Comment Request on Future Root Zone KSK Roll Overs. A bit of history on this document, I think I sent around something to the caucus before Christmas I believe, in early December, asking for comments on IANA's proposal. I received a lot of comments, from those comments I created this document. Since then, had a lot of good commentary in the document. Thank you everyone who commented in the document and also commented on list.

A few hours ago, I looked at all the comments on the document and made some proposed edits and I'd like to just go through the document, just start at the top and just work our way down. We are on a bit of time crunch. The ultimate deadline for this, getting this to IANA is January 31st. There's a bunch of things that need to happen before that can happen and that need to happen after we get down here. It needs to be stable for a week for the RSSAC to vote on it and these kinds of things. Paul, go ahead.

PAUL HOFFMAN: There are two things. One is, the deadline for RSSAC to respond in the Public Response Forum, where it would be noted there in such but the other is, for example, if RSSAC misses that deadline and still wants to give IANA advice, these Public Comment Periods are actually as we know in RSSAC sometimes, sort of open forever, that is, IANA won't say, "Nope, you missed the deadline, we don't want to hear from you."

It would be nice to try to meet the deadline but if RSSAC itself comes up and I'm speaking not as IANA but as somebody who works close to them, I know that the folks who are working on the key roll there are always interested in new ideas both from within and outside of ICANN.

ANDREW MCCONACHIE: That's good to know. I'd like to work -- we're working under the assumption here that this document will finish up in time for the Public Comment Period. Brad, go ahead.

BRAD VERD: I would agree with what Paul said but in context of this document, there's no reason we should miss the deadline of the end of the month and in order to do that, we need to get this document done in the next week or this week. Let's just focus on that.

ANDREW MCCONACHIE: Thanks. I'd like to propose that we just work through the document as I said, working from the top all the way down. Really, if we can't reach consensus on specific items with document, I'd like to suggest that we just strike them, maybe a minimalist approach to the document. Hopefully at the end of this meeting we'll have something that's mostly done, if not entirely done.

Maybe we can take a few things to list but as Brad said, we should really try to finish up by the end of this week, if that means -- if there's still something that's outstanding and we want to talk about it on list for a

couple days, by Monday or Tuesday next week we should have something to give to the RSSAC.

With that in mind, I'm just going to start at the top, unless anyone has anything, does anyone have anything else before I start going through the document. Brad, your hand is still raised but I think that's an old one.

The first comment here is from Duane, he suggests to strike this paragraph and my suggested edit was to strike this paragraph. Does anyone have an issue with that or should I just merge that? Okay, hearing none but, "Well, do it." I will strike this paragraph.

I'd had originally written RSSAC's Charter, that's kind of incorrect. I changed it to, ICANN's Bi-Laws. This is just a quote.

As I'm working through this document and accepting things, please raise your hand at anytime if you have comments you'd like to add.

This comment from Duane as well. This line on data analysis of potential breakage, potentially conflicting with some of the future advice in the paper. My suggested edit is to delete this. Is that alright?

DUANE WESSELS: My opinion hasn't changed.

ANDREW MCCONACHIE: Brad, go ahead.

BRAD VERD: I find it interesting that omit or we add risk assessment as out of scope. It seems to me that if there was a risk to the RSS, then that would be within scope of us to comment on. Maybe they were talking about a different type of risk assessment, I'm not sure but that seemed rather broad.

ANDREW MCCONACHIE: Paul.

PAUL HOFFMAN: I think the risk assessment here is the risk assessment based on the contents of the root zone, that is signing with multiple keys and different keys and such, as compared to the risk of the root service.

BRAD VERD: But aren't the connected, meaning if the keys were too big and you started breaking the root service, then that would be…

PAUL HOFFMAN: They could be related but there are not necessarily related. For example, there is a risk of changing algorithms that would probably not affect the root service per say, although it might.

BRAD VERD: It might if it was implemented.

PAUL HOFFMAN: Yup, I hear yeah. I think you're right. I think I'm being to nitpicky here.

BRAD VERD: This just seems to broad is kind of where I'm at here. I don't know what value that's adding, I guess? Why we're -- certainly communication and outreach, not something we would be interested in. We being RSSAC, risk assessment, yeah, I think so.

Maybe I'm reading that sentence wrong, they way it reads, "A broader set of issues, such as communication, outreach, risk assessment and postural issues may need to be addressed but are outside of RSSAC scope." I don't know, I have a hard time with the second half of that sentence, I guess. How are they going to know there are postural issues without -- I mean I guess users would be failing.

PETR SPACEK: Maybe, can we get back to this point once we are done with the rest. Maybe the next points will uncover that we need to -- we have had particular risks which we need to assess and then we will have more ideas as what to do with this particular -- I'm just wondering out loud. Maybe if we go through the rest of the document, we will find out that we didn't identify any particular risks we are interested, so it's pointless to put emphasis on it or maybe we find out that there is something and then it will be easier to decided later I think.

BRAD VERD: I'm fine with talking about this later, as we're going through it, this statement right here, you're essentially defining scope and by having

risk assessment and postural issues out of the scope of RSSAC, you're essentially putting that in a document stating that going forward, those are out of scope for RSSAC potentially and I think that's limiting and I wouldn't want to do that. Certainly, the communication and outreach I don't have a challenge with but yeah, happy to talk about it later.

ANDREW MCCONACHIE: We can certainly come back to this topic. If we do remove risk assessment postural issues and we just make it about communication and outreach, we can just change it to that because then there's no longer a list but we'll come back to this once we've gone through the rest of the document.

Moving on, Phases and Cycles. Section 3.1, a lot of discussion on this and pretty much everyone saying to strike this section. My edit is to strike this section, is there any opposition to that, please speak now?

FRED BAKER: That seems rational to me.

ANDREW MCCONACHIE: Thanks. Paul.

PAUL MUCHENE: I have no objections. I raised this point because I was a bit concerned that exposing the key for two years could maybe give an attackers some

leverage to play around with ways to exploit the key, so that's why I mentioned it. I'm okay if it's stuck out.

ANDREW MCCONACHIE: Okay, thank you for that, I will strike it. Moving down. I'll renumber these things later. Let's talk about the second paragraph of measurement. This was a comment from Duane. I had written that all root server operators had implemented RSSAC through data collection and Duane kind of rightfully said that they hadn't all fully implemented RSSAC 002 yet and also pointed out that this paragraph doesn't really offer anything new so we could just strike it. Any comments on that? I think Brad and Paul, your hands are old. Russ. Russ, I believe you may be on mute.

RUSS MUNDY: Too many mute buttons, phone and zoom. Sorry about that. I think that yes, striking is the right thing to do here because the measurement that I think is being described here is not really related to either of the metrics document or 002 because measuring the effects or state or results of the KSK Roll is something that has been up in the air item certainly from the SSAC perspective, since SAC 63 and SAC 73 and it's never, at least in my opinion, ever been really addressed in a complete sense.

There have been some efforts and so forth but it's never really had any sort of quantitative thing raised. I'm very glad to see the first paragraph [inaudible], but I think the second one is unrelated.

ANDREW MCCONACHIE: Thanks, Russ. Anyone else that has an opinion on striking this paragraph. Hearing none, I will strike this paragraph.

3.3 comments from Paul and Duane, disagreeing with the harness of this ton. Duane also just disagreeing with the paragraph. Would anyone like to keep this paragraph? This is the single paragraph under Section 3.3. Hearing none, I will strike this paragraph.

Section 4.1, this was -- or Russ, I see your hand is raised, go ahead.

RUSS MUNDY: Thank you, Andrew. I think we need to look again at the actual word construction in the first paragraph. I'm not sure that it expresses things correctly or reads correctly, it ends with, "Not relevant to a review of IANA's proposal for future one KSK rollovers." Is the one out of place? Anyway, we just need to make sure that that is reading correctly because I don't think it does at the moment. Maybe simple as change, looks good.

ANDREW MCCONACHIE: I see what you're saying Russ. I'm not sure that's the right change because it seems to just contradict the sentence previously. I agree, it needs attention. I get what it's trying to say but the comments are to the current plan before us and not future plans. And one seems out of place, now I understand. Fred, go ahead.

FRED BAKER: On 4.1, maybe I'm being pedantic but it seems like there would do well to be a sentence saying why this discussion of algorithms are important. It seems like, in the current plan, algorithm is considered separately from the key but a key is an attribute of an identified party using an algorithm.

At any time that you change the key, you're implying two things. You're implying what algorithm specified that key, if I have a 302 bit RSA key, that implies that I'm using a 3072-bit RSA algorithm and that I have a key that's that one. They're two things and they go in pairs; you can't really specify one without specifying the other.

My way of thinking, coupling them in any change also works and I don't understand the concept of changing the key or changing the length of the key without saying what algorithm it's a key related to. It seems like there's room for a sentence here that summarizes what I just said. The reason the key is important is because we have an algorithm, if you're changing the key, part of that is potentially changing the algorithm. The fact that they left the algorithm is just baffling to me.

ANDREW MCCONACHIE: Paul, go ahead.

PAUL HOFFMAN: Two things. Fred, you are unfortunately are technically incorrect with what you just said. The algorithm identifier for RSA does not have a key length, it is regardless of keys. IANA could change from RSA 2048 to

RSA 2049 or something else without changing the algorithm identifier because RSA is for all sizes.

The key length is only incorporated when change in the algorithm's for elliptic curves and there are technical reasons why that's the case but actually in all protocols, not just in DNSSEC, RSA is the -- you can change key lengths within that. In fact, there are technical reasons why you would want to do, in fact Verisign just showed that by them changing some of the lengths of the keys in .com without changing the algorithm identifier.

The other reason I raised my hand is, I'm going to have to leave unfortunately soon but Andrew, I think you're going to have a little bit of work to do on reorganizing the document because Ozan, if you scroll up just a little bit, we'll see that Section 3 actually is now one paragraph long and it's only a single concern.

Now, Section 4, where we're talking about other considerations, that might feel funny given that we only had one consideration up there. I'm just saying that once you start looking at this, you might want to look at reorganizing. Thanks.

FRED BAKER: Okay, let me come back if you don't mind. My issue that I was raising was that when you specify a key, it's a key related to an algorithm. If I gave you an RSA key and you were using elliptic curve, life would be really difficult. My point is, that when you say there is a key of a certain length, whatever length that is, it's for an algorithm and the two go together.

PAUL HOFFMAN: Sure, fully agree on that. I think that in the -- looking at the IANA document, they are assuming in the document that the next rollover will keep with the same algorithm, even if they change the key size. That would not be an algorithm change and they would say, "We're just changing the key size." I think what you're saying Fred is, that you would want them to say, "Also and we're keeping the algorithm." Say that out loud.

FRED BAKER: Yeah, very much agree.

PAUL HOFFMAN: Yeah, that seems like a reasonable thing for us to maybe find some words to say, "So that it is clear to the community, that the next change might still be a change in size only."

FRED BAKER: Or some future it might change both. Yup.

ANDREW MCCONACHIE: Sorry, I was just taking some notes there. Okay. It sounds like we want to add a sentence to Section 4.1 that states that in Subsequent Changes they may change this but for the next one at least, they're not changing it, differentiate between change in the key size and changing the algorithm generates the key. Ryan, go ahead.

RYAN STEPHENSON: This is touching back on the section 2, where Brad was discussing about a broader set of issues, such as communication and outreach, risk assessment and post rollover issues. I'm wondering, I know what he's thinking about from an operational standpoint, being a root server operator. I'm wondering if maybe risk assessment and post roll issues may need to be addressed, maybe a paragraph in the -- it would probably be like 4.2 and part of the other considerations? I don't know if that may resolve that Section 2 discussion we had.

ANDREW MCCONACHIE: Russ, go ahead.

RUSS MUNDY: Back for that one and the comment about algorithm changes. As those words get put together, we need to make the comment be, at least have it makes sense with respect to the Section 2.6 in the IANA Plan in which they specifically start off that section by saying, "We do not propose changes in algorithm or key length at this time."

They did make an explicit statement in the IANA Plan and I think it's fine for us to comment on it further but we just to make sure we don't look silly with what we say -- we don't want to infer that they didn't say something in their plan because they did.

ANDREW MCCONACHIE: Okay, how about in the beginning of Section 4.1 we just provide that reference that you just referenced and noted that they've done this and they've explicitly stated that they're not considering a change to key length or algorithm type right now, would that alleviate your concern, Fred?

DUANE WESSELS: The text proposed kind of already says that, where it says, "The RSSAC supports the plan's remain on the existing algorithm and key length."

FRED BAKER: And that's a good statement, Duane. What I was getting at, was whenever we talk about the key length or anything regarding the key, seems like the algorithm should be mentioned, it's a coupled attribute.

ANDREW MCCONACHIE: It says, "Existing algorithm and key length." Should we mention -- is there some other aspect of the algorithm we need to mention there. We could mention the algorithm specifically and the key length specifically, I guess. I'm not sure that addresses Fred's comment but we could name them.

BRAD VERD: I'm not sure I understand Fred's comment. I'm sorry, I'm trying. Can you help me Fred, understand what the concern is?

FRED BAKER: Yeah, I'm assuming that next time they decide they want to change the root key, they're going to start with this document and edit it in whatever way they need to and at that point, they might be going elliptic curve, might be something very, very different. There's no requirement that in some future key roll that it remain RSA.

What I would like to have clearly stated here is that, they key and the attributes of the key are related to the algorithm and specified by the algorithm. To say the key length without saying the algorithm, doesn't really make sense.

Let's bring this back to SSAC's comment I believe, George Michaelson's if nobody else, that gee, this document doesn't say anything about the algorithm and maybe it should.

BRAD VERD: The document specifically states that it's out of scope, right?

FRED BAKER: And I just really don't understand that. To say that there has been a decision to not change the algorithm, that's fine, that's a good thing. To say that it's out of scope, no it's not.

BRAD VERD: It's out of scope for this key roll, that's what they're saying, right? This plan is for the upcoming key roll and I assume and I would fully expect that should there be an algorithm change, there would be a other plan that would go for public comment and there would be a lot of

discussion about that and the implications of that. I just want to make sure we're not trying to boil the ocean with this one document here.

We are commenting on this KSK plan that's been presented, not future plans, this plan. Well I don't disagree with your comment, I'm just curious how it fits in to this KSK Plan, given that they have stated in this plan, that they're not doing an algorithm change, therefore, that's out of scope. I think it's fair for us to say what we've said around algorithm changes but I think we need to be careful when trying to comment on future rolls, because we don't know what they are.

RUSS MUNDY: If I could jump in a little bit here. I think part of the confusion is that some of us are reading the current plan as applying to only the upcoming rollover and I think that's generally what their intent is but when one looks at the introductory paragraphs and executive summary, it's not totally clear that that's the case.

They may mean it to be predominantly used for just the current one and any future ones will incorporate changes. I don't know that they actually say that in the plan itself. One could read it to say, "This is the plan that will be used in the future as well as for the upcoming one."

FRED BAKER: And that's how I read it. I expect this to essentially become an algorithm. This is how we roll the key.

ANDREW MCCONACHIE: Would we like to see something in their plan that says, for example, "When it comes time to change the algorithm, we expect a new plan to go for review?"

BRAD VERD: That seems reasonable and would cover all the concerns.

FRED BAKER: That works for me.

RUSS MUNDY: That would be good, yes.

ANDREW MCCONACHIE: I've made a change to the last sentence there, that paragraph. Does this address the concern?

FRED BAKER: Yeah, that works for me.

ANDREW MCCONACHIE: Thanks Fred. Does anyone have any other comments on this paragraph or cutting the text that it's replacing? Does anyone have any comments on Section 4.1? Great, hearing none we will merge that.

There's this errant one here that I deleted. I know there was some discussion about this sentence here, the sentence in Section 4. Are

there still comments on this sentence? Are people fine with it the way it is? Okay, thank you very much. Petr, go ahead.

PETR SPACEK: I have one question. Clear that the Section 4.1 is not basically approving, keeping the algorithm and key length for many future rollovers or not? I'm not sure myself right now after deleting the one case because Section 4.1 in my understanding says, that RSSAC is fine with keeping the algorithm and key length but the introductory paragraph before -- the very beginning of Section 4 says, that this now applies to all future rollovers, so I'm just wondering whether we should be more explicit that RSSAC is fine with keeping the algorithm once and specify explicitly that only for the immediate rollover, not immediate but the next but not five next rollovers or something?

ANDREW MCCONACHIE: I'm not sure if it necessarily says that, there's certainly no timeframe put into this statement now to where IANA must preform an algorithm roll. Do others want stronger language here? Brad, go ahead.

BRAD VERD: I don't know if Paul Hoffman's still on the call but going back and reading through the document as it sits now, Section 3 and Section 4 I think should be merged. I think you could put Concern/Consideration and then have 3.1 as Measurement, 3.2 as Algorithm Changes and I would actually strike this lead in sentence because you essentially already say it in the algorithm change.

You say that you'd like a plan in the future for changing the algorithm, there's no reason and kind of having this qualifying statement up here, especially if you merge 3 and 4. Just a thought. That's what I would do if it was my document.

PETR SPACEK: That sounds good to me. That addresses my concern but maybe I'm being too formalistic. Feel free to ignore that.

FRED BAKER: I would agree. Andrew, didn't we already ask you to merge these?

ANDREW MCCONACHIE: Yeah, we had deleted so much text that we were going to merge them anyways. I've done that in the document now, what Brad suggested. We just have Section 3 for Concerns. We have 3.1 which is Measurement.

BRAD VERD: I would make Section 3 Concerns and Considerations and then 3.2 is your Algorithm Change, see what I'm saying?

ANDREW MCCONACHIE: Yup.

BRAD VERD: Okay, you got it.

ANDREW MCCONACHIE: So, basically like that? So, we just have two subsections underneath Section 3 and then we have Section 4 for Conclusion. Okay.

BRAD VERD: While we're on this topic, that sentence leading into Section 3, I deleted a word in there, just because of those changes below.

ANDREW MCCONACHIE: Okay. I'm going to get rid of the word regarding as well. The RSSAC offers the following…

BRAD VERD: Yup.

ANDREW MCCONACHIE: Okay. A lot of edits proposed here. Russ, go ahead.

RUSS MUNDY: Thanks. There was one thing that I wanted to just bring up on this call that is very likely to…

BRAD VERD: Russ, can you talk into the mic?

RUSS MUNDY: Okay, let me try a different mic. A lot of hammering going here. It is highly likely that SSAC will include a request to see some further detailed planning information from IANA relative to this. I'm just raising it to make RSSAC Caucus aware of that and if the content feels that they would like to look other positional plans or additional information that IANA may produce with respect to the upcoming rollover, that that could be part of what the RSSAC ask for also.

I don't necessarily think that that's critical by any means, but I wanted to make folks aware of it so if they wanted to raise it, it would be coming from RSSAC as well as SSAC. I'm going to mute since there is a lot of hammering going on outside.

ANDREW MCCONACHIE: I guess with that comment it sounds like the SSAC will be talking a bit about more details, does anyone else have any comments on that or comments on the large set of changes that we just proposed to Section 3 before I merge these? Okay, hearing none, I'm going to commit these merges.

Heading back to the second paragraph of 2. I was actually thinking about this a little bit. Let me propose we do this. Basically, just get rid of that sentence where we qualify what RSSAC's scope is and just say, "Given this, the RSSAC limits its comments to its scope. The impacts, the proposed KSK Rollover timeline to the RSS. With that in mind, the RSSAC offers the following potential impacts to adopting a proposal for future root zone KSK Rollovers."

BRAD VERD: I think that's much cleaner, thank you.

ANDREW MCCONACHIE: Okay, thanks. Thanks, Duane, I see your thumb, your virtual thumb. Mukund, did you want to raise something about the document in general?

MUKUND SIVARAMAN: Yes. This is about the PDF document which was linked to the ICANN website post. When the last root key rollover happened, there were two ways in which resolvers got the new [inaudible]; one was RSC 511 and the other one was as part of the software, they did a software upgrade and got it.

Things like [inaudible] the supporting -- basically the measurements that were done during the time leading up to the root key rollover, whatever measurements that were recorded there, sent back by software which was literally recent, which already likely had the new root key. At the Bangkok ITF meeting when this was discussed, the key rollover had just happened and it was discussed, some of us felt that the success of the root key rollover may have been more because resolver software was upgraded, rather than all the resolvers getting via RSC 511.

Maybe RSC 511 was not tested that well, which I what I meant to say. It doesn't wide use, it doesn't widely implement it, that's for sure. There was no measurement that we really got of how -- why the root key rollover was successful. Was it because the root key was already there

as part of the software upgrade or was it because RSC 511 works really well?

In ICANN proposal, there is a timeline of three years of key root key rollovers and that is very good because that still gives software ample time to include new keys when they come up, standby keys when they come into the software as part of their upgrade cycle.

The standby key really is -- it's mentioned in a way that it seems like it would be available only through RSC 511 mechanics, it will not even be visible all the time. It may appear for some time and then go away although the key is still valid, although the key is still there, it's no longer part of the key set, once it's observed. It may be introduced at a later time but resolvers learn of it via the RSC 511 process.

I'm just wondering, there is mention of this emergency key rollover as well in the document and I'm just wondering, now do we test that, this work. For example, if there is an emergency key rollover and the standby key has been learned by all the resolvers by then, then the standby key can be used at the root key. How do we know that for sure? In case you have to do an emergency rollover, how do we know the RSC 511 works well and this is going to work?

What I'm trying to get at, from the last key rollover we really don't know how much of it was because of the upgrade of software which had the key built in verses discovering it via RSC 511?

ANDREW MCCONACHIE: Thanks for that. I see Brad stepping up to the mic.

BRAD VERD: That sounds like a measurement thing, which you just described. Do we need to add some extra language on the Measurement Section that we have in the document to accommodate that? "RSSAC looks forward to discussions regarding KSK telemetry measurements." I don't know how to word it but is that what you are asking for?

MUKUND SIVARAMAN: I don't know how we would measure it now. I don't know how this could be measured really. Whether a key comes via RSC 511 or via [inaudible]. There are also various quirks in the software, for example bind, it trusts -- basically encouraging you to use a RSC 511 key database verses you trust anchor appeared as trust anchors.

There are cases like this that measurement will not really show. It will skew measurements. The question is this, how well do we know that it's RSC 511 that worked well and made the last key rollover a big success and how well prepared are we for an emergency root key rollover if it has to happen?

DUANE WESSELS: I think those are really interesting questions and I agree that they should be studied. What I don't know is and maybe you're in the same boat, maybe these are not appropriate comments to make in response to the plan but they should be raised somewhere. I agree because I think those are very interesting. It may fall just to research to have to

do that work, rather than IANA who sees their roll as very operational but I would like to see that work done.

ANDREW MCCONACHIE: Russ, go ahead.

RUSS MUNDY: Thanks, Andrew. I don't want to say much about what SSAC is going to say but I'm sure a number of those issues will be part of what how the SSAC responds to this document, but I agree with what I think Brad's initial response, that you raised very important questions, they do seem to be related to measurement and I guess I tend to -- anytime we think about something of this nature, I remember what SSAC wrote in SAC 63, which is probably and I'm not sure how many years old, it's at least seven or eight, it maybe 10 and there's two specific recommendations in there talking about having some way to actually measure what occurs and as far as I'm concerned, that really hasn't been done.

I'm fully in agreement, that it's an important issue. I'm not quite sure what or how we should address it as the RSSAC Caucus in response to this plan but I'd be supportive if folks wanted to say additional things in the Measurement paragraph. Thanks.

ANDREW MCCONACHIE: Petr first and then Wes.

PETR SPACEK: Thanks. I also agree that this is an important question. I don't see how we could specify that in RSSAC's statement because I feel that the Section 3.1 already covers all the measurements, including this one. I think it would be just fine to go DNS and try to either design a protocol or design experiment. I don't think that we should expand the Section 3.1 more because we could spend hours and hours experiment proposals. I think it's already covered in the more generic Section 3.1, that's what I wanted to say.

WES HARDAKER: I think that that's valid, that the measurement already discuss but the concern --maybe the right thing to do would be to add a sentence to 3.1 that says something like, "We would like to encourage IANA to pass on this concern to ICANN or the ICANN Community or Board." I'm not really sure what's appropriate there, to reemphasize that the operational impact of not having a sufficient measuring system has already shown problems in the past and really needs more research and study as future rollovers happen.

PETR SPACEK: On this generic level, it's fine. We can put more emphasize on the existing Section 3.1 but I wouldn't go into specifics because again, we could be adding tons and tons of proposals. On generic level, sure, we can emphasize more need for more measurement and understanding of what's actually happening in the rollover.

ANDREW MCCONACHIE: I'm trying to wordsmith on the call and that's not always the best thing to do. If you want to send me a sentence Wes after this or just stick one in there, that might be you doing that right now, please do.

We have seven minutes left and I want to give people time to say any kind of general comments about this document that they have. I stated at the beginning of the call that it would be great if this document could be basically done at this end of this call and we did a really good job, thank you everyone. Are there any general comments about this document that are a bit more than just, we need a sentence here? Are people mostly happy with this document?

BRAD VERD: Down on the Conclusion I felt like we need -- oh, you already took care of it. Okay, great. Just based upon the changes we made above, we had to change some of the verbiage to make it sound right.

ANDREW MCCONACHIE: Yeah, I saw that, thank you. Anyone else, general comments on this document? Duane, go ahead.

DUANE WESSELS: I like the document. One minor nitpick, maybe the title should be updated a little bit to reflect that this a feedback to IANA's plan or IANA's request for comment or something like that. Overall, I like it a lot.

BRAD VERD: Wes, is that along the lines you're thinking or is that not close to what you were trying to say? I took the words from above, which is the consistent, predictable and deliberate, which is what we say should happen. In order to reach that, we're basically confident in these changes.

WES HARDAKER: Yes, I would say root telemetry mechanism or something. The general nature I think is fine and thank you for doing that so I don't.

BRAD VERD: Like that?

WES HARDAKER: Yeah, I mean we're not really putting in what we want them to do with that sentence but I don't know that we can really suggest an action. We suggest IANA be concerned too.

BRAD VERD: That's just a suggestion there, I don't know if people like that or not but I was just trying to capture what was being said on the call.

ANDREW MCCONACHIE: To address Duane's concern about title, can we go back up to the top of the document real fast? I changed it so that it's IANA's Proposal for Future Root Zone KSK Rollovers.

DUANE WESSELS: Yeah, that's good, thanks Andrew.

BRAD VERD: I got to signoff, sorry guys, I have a hard stop. I have to get ready for my next call.

ANDREW MCCONACHIE: Thanks, Brad. We have about three minutes left. Let's go down to Section 3.1 again, this is the last thing we have to talk about. Let's just stare at this sentence again and if anyone has any comments in the next three minutes, please make them. [AUDIO BREAK]

I'm not hearing any comments so I'm going to merge them.

DUANE WESSELS: I think you should merge it. My comment would be that it's kind of passive, it says, "Development should happen on root telemetry mechanism." It doesn't really say who RSSAC thinks should be doing that or who has responsibility for that. We probably don't even know ourselves yet. I just think in order for it to be useful feedback to IANA, they would need a little bit more direction then just a passive voice but maybe it's the best we can do, I don't know.

ANDREW MCCONACHIE: Either we leave it as passive or we call out a specific actor like the Community, the ICANN Community. We can be vague about which actor we wish to take that action.

DUANE WESSELS: Yeah, or we could say something like, "IANA should ensure that it gets built." Maybe we just leave it as it is for now. Yeah, something like that.

ANDREW MCCONACHIE: How's that, then IANA is just doing investigating, they're not actually doing any development?

WES HARDAKER: Promote might be another good word.

ANDREW MCCONACHIE: Promote the development of?

WES HARDAKER: Yeah but I'm not picky either, just thinking out loud.

ANDREW MCCONACHIE: So, I'm going to merge the sentence, we've come to the top of the hour. We're basically done. I think it's fair to send this to the Caucus again for a couple of days. To answer Fred's comment in the chat, officially for the RSSAC in order to vote on something, it needs to be stable for seven

days but in addition to that, I think it's important for Caucus members to have a final say on it.

What I'm going to do after this call is send a note to the Caucus, basically giving the outcome of this call, saying the group has finalized this document, please review it one last time and give folks a 48 hour deadline to do so and then the document will be stable Monday or Tuesday of next week, that's the plan. Thank you everyone for all of your help, we got a lot done in this single hour, it was really productive, thank you.

WES HARDAKER: Thank you for your work on it, Andrew, you're the primary pen.

ANDREW MCCONACHIE: Thanks, everyone. Have a good day, wherever you are.

[END OF TRANSCRIPTION]