ICANN70 | Virtual Community Forum – RSSAC Work Session 1
Tuesday, March 23, 2021 – 09:00 to 10:00 EST

OZAN SAHIN: Hello and welcome to the RSSAC Work Session 1. My name is Ozan Sahin and I'm the remote manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior. During this session questions or comments submitted in the chat will only be read aloud if put in the proper form as noted in the chat. I will read questions and comments aloud during the time set by the chair or moderator of this session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To read the real-time transcription click on the closed caption button in the Zoom toolbar. With that, I will hand the floor over to the RSO Work Party leader, Ken Renard.

KEN RENARD: Thank you, Ozan. This is Ken Renard and welcome. Thank you for joining us today and I wanted to start off by giving an overview of the document and the Work Party progress. There's quite a few folks that haven't been part of the Work Party all along so I just wanted to give a

brief background of where we are and what we're doing and then we'll roll into some of the document changes, discussing those and hopefully finalize with some work. Then, try and get this document moved towards publication.

To review about this Work Party. This Work Party has been going on for almost a year now, it started in April of last year. It's gone in many directions, we've boiled many oceans but we're settling on a simplified document that's being pulled up right now.

This Work Party on Rogue DNS Root Server Operators grew out of the RSSAC037 document where it describes scenarios of where a root server operator might need to be removed from the list of root server operators. One of those scenarios was that a root server operator goes rogue so this Work Party was spun up to try to further define or further exemplify what rogue meant, what the RSSAC Caucus can contribute to the future governing body as far as a foundation for rogue behavior, what it is, what it is not. What we've come up with here is that really determining whether a root operator is rogue is a very difficult and subjective decision where intent of an action is a very big part of it. So what we do in this document is we outline our view—RSSAC Caucus' view—of what actions might be rogue. Some exception conditions like, for example, testing and temporary conditions.

We list a few examples which are certainly not exhaustive. They're objective and subjective scenarios of potentially rogue behavior that could be used for this future governing body to, again, determine intent and then potentially invoke removal of an operator. So far we've been

looking at this—at least I have been looking at this—from two viewpoints. First viewpoint is the main one which is how do we protect the root server system from a RSO doing something bad or rogue? Given that the root server governance body may decide to add or remove root server operators for capacity reasons, for other reasons, we know that this has a potential to definitely change the landscape. We wanted to set down and look to see what are some criteria, what are some examples of what could potentially happen especially if the list of root servers were to grow and essentially some nefarious group were able to come in and be rogue or one of the existing operators went rogue.

The other viewpoint we're looking at this is from existing RSOs how do we protect ourselves from mistakenly being identified as rogue? So looking at both sides of that and trying to define it, again, in a way that protect the root server system but also protect RSOs from being mistaken. With that, I'll ask if there are any questions so far and we can discuss any motivations or background of the Work Party before we go into discussing some of their latest changes to the document. Looking for hands and don't see any yet. Okay.

All right. So, the Work Party Core Writing Team met last week to discuss some of the latest comments and directions that the document's going to go. So wanted to go through that list, discuss what we talked about and get more feedback from the wider community here.

If we look at the introduction here, the second to last paragraph, the part that's highlighted on there. The recently added sentence there, that this document focuses only on the activities on IANA-designated

RSOs. This grew out of several things that we've talked about previously but the idea here is that we're really trying to focus on only the actions of RSOs as they're designated by IANA. If somebody is, let's say, intercepting packets and running a root server that's not an officially sanctioned—or you could call it an illegitimate root server—that's not what we're talking about here with respect to rogue. We're only talking about existing IANA designated root servers doing something bad. So the question here is with this last sentence of the second to last paragraph, again highlighted here, does that sufficiently capture that those activities and are there any comments on it? Go first to Paul.

PAUL HOFFMAN: I wanted to clarify something that you just said, Ken, to make sure other people who are reading this understand. You said that this doesn't apply to people who are intercepting packets and acting as their own root server. The "and" there is incorrect, it should be "or". That is this doesn't apply to somebody who is intercepting packets because we can't affect that. But it also doesn't apply to somebody who has said, "I'm your root server," and somebody believed them. That's a fairly important distinction in that anyone can say, "Use me as your root server. Stick this in your configuration and I'm your root server," and we can't have an effect on them either. So it's both of those cases, it's not a combined case. Thank you.

KEN RENARD: Thanks, Paul. That's accurate because neither of those scenarios are actions of an IANA designated root server operator. Any other comments on that? If that sufficiently captures things, great. If there's any other thoughts, any other text, or anything that we should add in there, like to hear suggestions.

The next part is the second paragraph of section three and that is highlighted here by this comment. So we're talking about descriptions of a rogue operator, things that a rogue operator might do, and specifically calling out accidental mistaken temporary conditions that are reasonably remediated or not considered rogue. From there, we have the idea that any future governing body has, albeit a difficult task, of determining the intent behind a rogue action.

So was this action accidental, mistaken, temporary, or was this something done with the true intent to deceive or negatively impact the query source? That makes sense in my head but I'd like to hear other people's opinion. Is this capturing sufficiently the idea that the governing body is going to actually make this determination, determine intent in some fashion, and really make the call of whether or not these actions by a RSO are actually rogue? Looking for any thoughts there. Okay. Without seeing any, I will close that out.

With any of these comments, if you don't chime in right away, please feel free to put something in the chat and we can come back and discuss. If you're a member of the RSSAC Caucus, you can also comment in the document as well as comment on the RSSAC Caucus mail list.

Now we're going down to let's see just before section four. Previously we've described a couple scenarios that are objective scenarios where it's something measurable, something happens and we can determine, we can say that this type of behavior could qualify as rogue. Paul?

PAUL HOFFMAN: Ken, you skipped a comment—I think an important one—that was also up above from Andrew McConachie.

KEN RENARD: Thanks. Okay. Our non-RSO responses and activity. So these are two sides of the same issue. Let me look at that one. Let's come back to this one. Thanks, Paul. Andrew, you want to talk?

ANDREW MCCONACHIE: Yeah, thanks, Ken. The comment I made there, I mean it could just be in the way that the sentence is written and maybe I don't understand but I just didn't understand how this, the last sentence of this second paragraph here in section three squares with what we talked about previously. The sentence of, "This document only focuses on the activity of an IANA designated RSO." So maybe there's just some clarification that's needed there but it seemed to me rather contradictory.

KEN RENARD: Again, it's really the same issue. It's basically saying that in the introduction, what we had just talked about—let's say that there is somebody intercepting packets and providing responses illegitimately on the behalf of an RSO.

WES HARDAKER: Ken, if I may?

KEN RENARD: Please.

WES HARDAKER: I actually think Andrew's spot on here and it's not that this sentence is wrong. This sentence is right. This document has suffered from the typical feature creep, in a good way, where we're talking about non-RSO responses but yet in the original introduction we say we're only talking about RSOs. What we need to change is not here, is actually the original introduction sentence that Andrew is highlighting. We're not just focusing on the activity of IANA designated RSOs if we have an entire section devoted to what happens about other people.

KEN RENARD: Thanks, Wes. In my mind, there are two parts to this. Let us consider somebody that's intercepting packets to and from an RSO address and providing responses. So one part of it is we are not going to determine whether that person is rogue or not. The other part of it is, given that

that person exists we are not going to use that person's responses when judging the actions of an RSO. Given that thought, if you could help me wordsmith this and make it into something reasonable to express those two different concepts. Paul.

PAUL HOFFMAN: Ken, you've just given two possible ways forward. One is that we reword that sentence or two in the introduction to only limit it to actors who are not intercepting, and then we leave this and section four. It seems like that the other possible action is to stay with that intention, remove this, and remove section four. Section four I think is there and I don't want to speak for other people but I think the history was section four was there because there was some concern that if responses are getting intercepted and being changed in a way that would look like rogue, we wanted to make sure that somebody who was evaluating rogueness wouldn't come down on the RSO for those responses from somebody else.

I know I had expressed at one point that seems pretty far-fetched if we can tell that those are intercepted responses. So the folks here need to decide which is the better way to go. Leave in section four but then make the introduction much more narrow about who we're not talking about, or get rid of section four on the assumption that somebody who's evaluating rogueness when they're told, "Oh, no that's actually not a response from the RSO," wouldn't say, "Well it seems like it is to me so I'm just going to punish them anyways." Thank you.

KEN RENARD: Yeah, I lean towards leaving section four in there and rewording the introduction to say that we are not judging that interceptor as rogue and we don't want his responses to be used in the judgment of a real RSO as two separate concepts. Wes.

WES HARDAKER: I'm madly typing away. I tried to clarify it here because I quickly reread both the introduction and section four and section four is really basically saying out of scope. It's important to think about but it's out of scope of this document. My attempt at rewording that sentence—and I left the original one in instead of striking it—was that this report addresses non-RSO responses. Don't we actually want to say it addresses RSO responses although we discuss responses that may have been perceived to have come from an RSO but did not actually come from an RSO in a later section? I recognize that's wordy and very quickly typed but we are attempting to say what is rogue behavior of an RSO but we do highlight that there are times where … And this is what section four really says, there are times where a packet may be received that—going down to the super technical in the weeds level—a packet may be received that looks like it came from an RSO but actually didn't and that that's out of scope.

KEN RENARD: Right. I don't know if that solves the potential confusion with that in the introduction.

WES HARDAKER: Andrew, I'm looking for your hand.

ANDREW MCCONACHIE: Yeah. So, Wes, I think you have addressed my confusion. I raised the comment because I genuinely didn't know what the intent was and I was genuinely confused. Now after listening to this conversation I think I understand what the intent is and, Wes, I think your new language there in the section paragraph of section three resolves my confusion, so thank you.

KEN RENARD: Okay, I'm thinking along the lines here if we change the introduction to such that this document focuses only on the judgment of IANA designated RSOs. So we're only judging IANA designated RSOs but we're acknowledging and we're saying later that we want to exclude these non-RSO responses from that judgment. All right, I'm going to propose something here maybe after the fact stating such that we're only focusing on judgment.

PAUL HOFFMAN: Ken, if I might, before you start typing, this document is not about judging, this document is about letting somebody else judge so I don't think that that's exactly the right word.

KEN RENARD: Yes, I agree and if there's something that you can think of to replace that last sentence of the second to last paragraph of the introduction, basically what you've highlighted in your comment in section one … I will work on that two, yes. So this document does not judge, does not tell how to judge it just tells, "Hey, somebody else is going to judge," but yeah we're not making a comment about that non-RSO responder. We're not calling that non-RSO responder rogue. Okay. So I think we can wordsmith on that unless anyone else has thoughts, you can put it in the chat or feel free to raise your hand. If we go onto section three, descriptions of a rogue operator and we talk about a couple objective scenarios and we have here a list of five scenarios that Paul contributed and we have titles for them. These titles are somewhat placeholders, so if the group can look through these objective scenarios and suggest better, more accurate, more precise titles, I think that that would be very helpful. I think these titles are necessary for document readability to get the brief answer and look through this document quickly.

The next part is the two subjective scenarios that we talked about here and we have, number one is intentionally degrading service and number two is currently struck out. It was called reduction and trust. I'll explain the idea here and we're trying to come up with a good way to describe this. We've so far failed to describe this in a way that's really precise. If anyone has any last thoughts that can really describe this in a precise way, we can offer to put that in here, otherwise we're going to remove this second example.

The idea is that an RSO is going to potentially make statements or some actions but the purpose is to reduce the trust in the overall root server

system to try and degrade user confidence in the system and maybe get people to not use it. That's something rogue. That's trying to undermine the entire RSS.

On the other hand, we have the idea that an RSO should be able to speak legitimately about criticisms of the RSS for the purpose of making it better, for the purpose of identifying problems that can be solved. Without a good way to really delineate those two different sides of it, we've basically given up and said we are not going to try to describe it here. So if anybody has thoughts on the topic or potential scenarios that could help us more precisely describe this in a document that won't be misread or misinterpreted later, love to hear your thoughts. If not we can just remove this from the document altogether. All right. I'm going to go ahead and hit the delete button.

Okay, onto the next topic is down in the recommendations section. The original thought here—you can read the struck-through text there—was that we recommend that the governing body define a process for determining intent and eventually coming up with the rogue designation and enough rogue and enough supporting evidence to eventually remove an operator. We looked back in RSSAC037 and those procedures are actually pretty well defined right there so that recommendation is essentially already done. The other thoughts of recommendations were to define a complete list of rogue behavior which seems pretty open-ended and not really feasible. Detection of rogue techniques or detection techniques to determine rogue really are spelled out as the responsibility of the PMMF, Performance Measurement, and Monitoring Function.

Mitigations are pretty well captured by the SAPF either giving a reasonable time frame for an operator going rogue to correct themselves or be removed from the system. So the idea from the core writing group was to actually remove the recommendations section altogether. We don't need to recommend anything and any thoughts on removing the recommendation section? All right. Pretty quiet group today. Please feel free to speak up.

WES HARDAKER: I'll avoid raising my hand, but I agree if we don't have a recommendation then we're just writing an advisory document and I think that that's fine.

KEN RENARD: Okay.

WES HARDAKER: I don't know what we'd recommend other than don't be rogue, right?

KEN RENARD: Yeah, well this is to the future governance body, so we hope that they don't go rogue but, yes, I agree. This is an advisory document from an advisory committee and it's sufficient that we don't have a recommendation. Paul.

PAUL HOFFMAN: This is Paul Hoffman wearing my ICANN Org hat here. If there are recommendations there is a whole bunch of process that we who work for ICANN have to follow even if the recommendation is trivial. I am happy to not see recommendations here unless of course we really had some but even if there was something that said, "Don't be rogue," or whatever the amount of work that we have to do to respond to recommendations and it goes to the board and it goes to other things, so happy to not have this here. Thank you.

KEN RENARD: That seems useful, and without saying anything, I think we'll just take the advice of the core writing group, and since there's no other comments I'll go ahead and remove that.

The last piece here was the Appendix A. So, in the framing of rogue operators and the framing of what operators should do and shouldn't do, we relied on the guiding principles of the root server system and root server operators which was initially defined in RSSAC037. We included that here as an appendix since it was referenced. Since then, it was brought up that maybe the RSSAC itself wanted to publish these principles in a separate document, thus we could just refer to it. That recommendation is being taken up by RSSAC and there are plans to publish these guiding principles in a document. So the advice here for the Work Party document is to actually remove Appendix A and simply refer to the RSSAC published document.

Seems very reasonable, makes us more concise of a document. The only thing that this does is it just puts a temporal dependency on the referral to this other document would just need to be published or at least known what the title would be before we can publish this document and I think that's okay. Does anybody have any concerns or comments or thoughts about removing this appendix and referring to the other document? Okay.

Okay, there's a comment in the chat. I would like to suggest this Work Party make a recommendation of increasing the diversity of RSO instance in a given country or area in avoidance of that the users in that area heavily rely on one or two RSOs which could be rogue. I hope this recommendation will encourage more RSOs to deploy more instances. Okay. The thought that any point on the Internet certainly doesn't depend only on the RSOs that are only close. Any instance of any root servers is available to anybody on the Internet such that if any root operator goes rogue—even if it's one instance or several—the entire letter, that entire root operator is subject to removal based on being rogue.

So if that leaves 12 instead of 13 root server identities that's perfectly fine and the root server system should completely work as it does. I will let Paul Hoffman speak now.

PAUL HOFFMAN: So it would be good if you brought this to the mailing list and not just for the discussion here. I can see both sides of the argument, that is, of

course, we are always trying to increase the diversity of RSO instances. But I can see two sides of the argument where simply increasing the number of instances could in fact allow more rogue operation instead of less. But certainly, we would hope that it would give people more opportunity to get to non-rogue root server operators. Again, we're assuming that rogueness is going to be exceptionally rare. Once an operators caught being rogue they're not likely to remain an operator really long. So Di, if you can bring this to the list we could have some discussion on that, that would be good. It may be that it goes in here because we're trying to avoid rogueness, it may be that it goes into another document where we're talking about the effects of having more instances that would be good as well. Thank you.

DI MA: Hi, Paul, can you hear me?

KEN RENARD: Yes.

DI MA: Paul, thank you very much for your suggestion. The reason why I put for this issue is it seems to me that the distribution of root server instance worldwide is not on [balance]. So in some areas, there are many root server instance, and in some other these instance are quite few, so maybe I think this suggests that you could encourage more diverse deployment of root [name] server instance. Yes, we absolutely could

bring this issue to mailing list to cover more insights in the coming future. Thank you.

KEN RENARD: I see how if an operator were to go rogue, that's one less or some fewer instances or just an entire operator being removed. I just think that that's somewhat of a mostly independent of RSO distribution. But, yes, so please bring that to the list and we can discuss. This document is more about how do we identify a rogue operator, what activity constitutes rogue, and how those things will play out in the process.

Okay, so those were the major changes that were made to the document from the core writing group. The document itself is becoming much more stable. We're nitpicking on some of the details, so we've had a few comments here during the course of this meeting that's been very useful. I guess what I'd like to do is open us up to any additional comments overall about the document. Is there something that we're missing, something that we shouldn't have in here because at this point we're mostly just cleaning up the document and getting it ready for a formal review by the Caucus?

Any further thoughts? All right, so those are the only things that we really wanted to cover here, and again I would encourage anybody to take a look at section three, the numbered sections there if anyone has any further thoughts on those titles would love some suggestions. Next steps would be to clean up some of the comments that were brought here today and I think at our next meeting we're going to start the

finalization of this document and just editorial changes and getting it ready for going through final Caucus review. There are no other comments I can turn us back to Ozan and maybe we can talk about the… I don't think we have a next Work Party meeting scheduled yet but it would be approximately a month. Ozan.

OZAN SAHIN: Hi, Ken. Thanks. This is correct, we don't have a next meeting scheduled yet but it will possibly be on the week of 19th of April. So if there are no other comments thanks everyone for joining today and have a great day.

JEFF OSBORN: Nice job, Ken, thanks. Thanks, Ozan.

KEN RENARD: Thanks, everyone.

OZAN SAHIN: Support colleagues, can you please stop the recording?

[END OF TRANSCRIPTION]