

---

SUE SCHULER:                      Okay, thanks. Okay, Jim.

JAMES GALVIN:                      Okay. Thanks, Sue. Thanks, everyone. This is our DAAR discussion group, here, from the Registries Stakeholder Group on the 20<sup>th</sup> of January. I am Jim Galvin, one of your co-chairs. I do see that Kristine is with us, too, another co-chair, so we are good to go. Our agenda for today, as reported in the probably much too recent past, we'll look the spreadsheet here very quickly. I suspect that most of the substantive discussion we'll have today is to dig in, again, to discussions of groupings in our type two category of TLDs.

We do have a related topic that we can also get into if we happen to get there, which is talking about how to represent actual mitigation as part of the DAAR reporting. We touched on that topic a few times along the way, here. Of course, Sue has added for us that we do need to have some ICANN67 planning, just to call out what we have going on there and our options. With that, let's jump right into the spreadsheet, here.

Thanks, again, to Dietmar. I mean, there are a few among us who dug in, here, filled out the spreadsheet, and added your entries. Thanks to the people that did that. But then, Dietmar went in and just did it for everybody and filled out the rest of the sheet. That was just awesome. I think that really was our intent, here, in this. It doesn't have to be the perfect answer right now. It really is just a first cut. It's okay if we get a few wrong. We're really just looking to have Samaneh cut across this data, make this split for us, and show us all of the TLDs split only by

---

*Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.*

---

whether they are open or not. And then, let's get a look at what that data looks like.

We did have some discussion up to this point about a subtype under type one. We had some categories there so we have a bit of a proposal for what that looks like. This way, people can make a point of looking at what Dietmar did and giving some real consideration to whether you agree with that or not.

And then, we can perhaps have another discussion about those particular groupings and whether they're the right thing. We're not using them right now with what we will give to ICANN. But obviously, our intent is to move forward with an experiment with those entries also at some point, here. We just have to pick when we're ready to ask for John and Samaneh to look at that for us. Oh, I'm sorry. I just saw the request in the chatroom. Thank you, Rick, for posting a link to the spreadsheet for Matthias. I'm sorry about that. Okay.

Again, the spreadsheet is there. I'm looking for people. If anyone has any comments or concerns about it, I'm watching for hands. Otherwise, the action here is that Kristine and I will take this sheet and strip it down to just the domain name and the type one or two designation. We'll certainly take off the subtype information and the "under 100" column, there, and ask her to run a cut across the data based on that type one or two, and then ask at what point they would be able to bring that to a meeting to show us the results.

Ideally, we can get this spreadsheet out to them today or tomorrow. With any luck, maybe she'll have it next week but my guess is that she'll want

---

at least two weeks. And so, we can plan to have a meeting with John and Samaneh in two weeks. We'll leave it to them to tell us when they want to do it. We'll let her take whatever amount of time that she needs or wants to do it.

Then, we'll let them come back and talk to us about that. Between now and then, we will continue our discussions of these subgroupings in the two categories as our agenda for the next couple of meetings, plus whatever else comes up that we need to dig into.

Any objections to moving forward with that particular action and passing on the spreadsheet? As Kristine had said in the e-mail, we'll put all of the proper caveats on it about, "it's just an experiment, "please don't republish," "don't use this anyway." Obviously, before we would expose any kind of designations like this, we really would need to go through some kind of process to confirm its accuracy. We want to be careful to be correct, there.

Natalia, please feel free to just update the entry. You're observing in the chat that you'd like to see that different. Please do feel free to make that change, whatever you need to do to make that right. Okay.

I think, with that, we'll go back to the agenda and we'll move to a discussion of the category two groupings. We'll leave the category one groupings as they are in the spreadsheet at the moment. Let's have a bit of discussion, here. Let me see if I can set up this discussion. I said a few words in the e-mail message that I sent earlier this morning in the agenda. This is something that Kristine and I have just been talking about. This is just to promote some discussion, here. It's potentially a different way to

---

think about this. To date, in our discussions, when we talk about mitigation strategies, we have actually casually suggested to ourselves that one option to think about is being grouped according to the mitigation strategies that are done. There might be collections of them or sets of them in some way; sort of the same concept as to what we've done with the type ones. We tried to create groupings of registration models that we could then put TLDs in for that to make sense.

A suggestion that I have, though, is that I'm a little concerned that it'll be a little harder to divide up our mitigation methods into groups that we could use to categorize TLDs. Part of the motivation for that is that there really are a wide variety of things that we engage in in applying mitigation. And so, it becomes a question of, "How much of that do we really want to expose?"

We have this concept of actually taking action and different things that we might do. "Takedown" is the obvious thing but there are other steps that we take to lead us to acknowledging that a particular domain name has abusive behavior and needs attention. It worries me a bit about exposing all of that. Maybe we want to be a little more circumspect about keeping some of that to ourselves.

And then, in thinking about it, what else could we do instead in how to divide up the TLDs? There is a lot of discussion about, "What is DNS abuse and what does it represent?" There is a certain amount of breakdown of abuses that are visible based on the feeds that DAAR gets that it uses.

And of course, there's a certain definition of DNS abuse as represented by our contracts and what's in them. And then, we have this recent

---

posting of a DNS framework that quite a few registries and registrars have signed up for.

It has its ideas about DNS abuse, essentially, breaking them down into three categories of things that are known based on contracts, things that are generally accepted as best practices by some segment of the community, registries and registrars, and then a spot for individual registries and registrars that might do unique things for whatever reason they choose to do that.

So, rather than looking at what we do for mitigation, as suggestion here, open for discussion, is: why not suggest that ICANN continue the path that they're on now and instead of dividing up the type twos into categories, after we look at type one versus type two, let's just go back and gather up all TLDs and look at the individual presence of abuse and presence of types of abuse. We have the definitions that are in our contracts. We can leverage off of that. We can let them leverage off of the feeds that they get, similar to that they have already decided that they'll pull out spam separately.

But why not go down the path of showing the TLDs in an ordered showing, based on the volume of abuse that's the volume of different types of abuse? You would have a separate chart for each type of abuse. Let's take a cut across the data, look at that, and see what that looks like.

That's the suggestion, looking at types of abuse, which they do already sort of do, versus us trying to go through the process of looking at mitigation methods and categorizing those, since that is something which is not all public. The registration model stuff really is mostly public. It

---

necessarily has to be, at some level. You can't buy a name if you don't know what the registration requirements are. But the mitigation methods would not be.

I'm not seeing any hands go up. That's an overwhelming idea. No reactions. Okay, now I'm just vamping and filling in the space. It's like being on a radio show. Well, maybe this is something to take to the mailing list and see if we get any disagreement or discussion about it.

But it might be worth, if nothing else, that, similar to when we do a cut across the groupings that we've created for the subtypes in category one, we just go with the same thing and ask or a similar experiment, at least, from Samaneh so that we could at least see what the data looks like and then make a decision. I mean, we don't have to make a decision, here. Really, it's just a question of whether this would be something interesting to look at.

Matthias has a comment in the chatroom. Right. "DAAR is not showing abuse. They do not check for false positives in the DAAR data." Well, that's true. They're only representing the data that they get. That's part of the messaging that has to come with what DAAR is and what it shows. I mean, you're right, Matthias. DAAR is only as good as the data feeds that they get and the data feeds have their own set of issues.

KRISTINE DORRAIN: Jim, am I unmuted?

JAMES GALVIN: Yes, I hear you. Kristine, please, go ahead.

KRISTINE DORRAIN:

Sorry, I didn't mean to interrupt. I wasn't sure if I had to push the magic star or whatever. Sorry about that. I have a question about something you said. I've been really pondering it, actually, since we talked yesterday. When we talk about the check going crossways across the different types of abuse, help me understand how what you're proposing now is different than what they currently do.

I believe what they do right now is they take all TLDs. Well, right now I think they're grouped by legacy and not but they take all TLDs and they do a pie chart, as I understand it, that shows how many are each of the four types, plus spam.

So there are five sections on each pie chart. If we take out the spam pie chart, which we're hoping to see at January 31<sup>st</sup> – I'm looking forward to that – then the pie chart should only show the percentages of the total of the four. Unless I'm misunderstanding? Help me understand how what you're proposing is different from that. Thanks.

JAMES GALVIN:

Actually, it's not at all, Kristine. I apologize if that wasn't clear when you and I were talking. I thought I had tried to say that here, too, but maybe I said it in passing, about letting them continue to do what they are doing and not trying to invent anything new on that side. Let me just state that very clearly. You're absolutely right. Let them continue to do the breakdown based on the feeds that they get. It would be nice if they could break it down further but they can only break it down based on what they can see. That's all they get.

---

I did want to offer one other comment of clarity, here. With the spam stuff – and maybe I'm wrong, and so it would be helpful if someone would clarify this for me – I didn't think they were removing spam, per se. They were separating it out as its own thing so that there was a way to show the rankings with all of the feed data, absent the spam data. And then, they would still be showing all of the data with spam included in the rankings in that way. So I don't think they were eliminating it. They were just allowing it to be called out and showing data without it included.

KRISTINE DORRAIN:

I agree. I think it was going to be two separate tables or a pie chart. I'm not entirely sure. That's part of the reason that I'm looking forward to seeing it – because I can't visualize how it is that they've made this change so I'm very eager to see if they've actually made a meaningful change or whether whatever they did makes no difference to the outcome.

Thanks for the clarification. I admit that it was probably entirely my misunderstanding because I think I was going into it with the idea that you were proposing something different so my mind wasn't hearing that it was not something ... I apologize for that. Thanks.

JAMES GALVIN:

No, no problem. Clarity is always good. Actually, maybe this issue about spam brings to mind something for me, which is that Samaneh never actually showed us what that would look like so we never actually got an opportunity just to get a sneak peek at what they were going to do. I never really thought about that particular point, before, but it stands out for me at the moment.

---

Now, I'm feeling a little sad about not having gotten that opportunity to see that before they're just going to publish it. I think that's probably something to keep in mind in the future. I mean, obviously, we're past doing anything about it this time but we should try to encourage Samaneh to let us see what stuff is going to look like before it goes up, since this is supposed to be a good-faith working relationship, here.

I saw a comment from Gigi in the chatroom that she thought it would be interesting to look at the data and let them continue what they're doing. I think the most important ... Maybe there is a slightly nuanced distinction about what I'm proposing versus what they did before. One is that since they're eliminating the legacy versus new gTLD distinction, and then also keeping them, having them not separate out ccTLDs, okay? That a TLD, is a TLD, is a TLD and the data should be shown in that way. So DAAR should focus only on the abuse that they know about and that they can pull out and separate.

They should just put all TLDs together and that's the way the data should look. We're asking, at this point, for an experiment in type one versus type two. I imagine a future experiment where we will be asking them to do the subgroupings in the type one when we're ready for that and we're satisfied that we've got a nice set of groupings that we can use.

I hope all of that was clear. If anybody has any questions about what I just said, it would be good to ask those and put it up there. Okay. This is going to be a short conversation today if we're not getting any objections or any other magic ideas. Maybe we just need to let people have a chance to think about that. We can bring it up again next week and also be prepared to talk about it with Samaneh when she's ready to join us for

---

their next meeting, once they do the split on the type one versus type two.

I'm going to move to talking about representing mitigation again, then. Let's just touch on that topic to refresh people and see if that brings anything to mind. One of the things that I think is important here, for us as registries, is that I have a bit of concern about the longer-term consequences of separating out registration models and then, in fact, being able to demonstrate ... I'm expecting the data to somewhat naturally show that any kind of preregistration step that you take in order to verify all of that is going to reduce the amount of abuse that's visible.

And so, the overall quantity of abuse will be much lower in the type ones versus type twos. I'm a little cautious about that being something that comes up. With that in mind, we should all be concerned about the pressure that will come to reduce abuse in the type twos, in the open TLDs. What do we want and how do we want to deal with that?

That's the motivation, in my mind. It has always been my motivation, this idea that we need to find a way to represent the fact that we actually do mitigate, and that any preregistration step that's taken is just one example of a mitigation method that has a certain effect and it actually is helpful in, perhaps, certain kinds of abuse. It'll be interesting to see what abuse does show, there, and what abuse doesn't show on the type one side. But I think that it's not the only method of mitigation.

The fact that there are those among us, registries and registrars alike, who are proactive about addressing abuse and our ability to represent that and have that be visible in some way, I do see as something that we

---

need to examine and look for a solution to, and to get that to be part of the DAAR reporting, also, in some way, for them to show that mitigation is happening.

This is partly in response to the messaging that we're hearing on the other side, which is that there is a systemic abuse problem. I think that we all agree, and we know for ourselves, that the problem is not systemic. It's actually fairly localized, for some definition of local. I mean, there might be regional localization.

Certain kinds of abuse lends itself to certain kinds of places. Sadly, there are some players who are not as good about mitigation as others, both among registries and registrars. We're aware of that and this data is probably, eventually, going to call some of that out and make some of that visible. But it's because of that that we are all being painted with this brush of being bad players. One of the ways to ...

KRISTINE DORRAIN:

Jim, can I get in the queue when you have a minute?

JAMES GALVIN:

Yes. And so, one of the ways to get away from that is to be able to show that mitigation is active and we are doing things. This is why this discussion keeps coming up, or why I at least keep bringing it up. I'm actively trying to think about what we could do that could also be incorporated into the DAAR website and the DAAR statistics.

It's somehow representing that registries and, ultimately, registrars, assuming they're still going to go down that path of including them in all

---

of this too, could also then demonstrate that mitigation is happening and we should be able to get credit for that in some way, at least in the community's eye. With that, Kristine, go ahead, please.

KRISTINE DORRAIN:

Thanks. This will probably be my last remark before I started heading down to my underground to get to the plane. I want to throw an idea out there that I have not proposed to you in the past and I have not proposed to this group, I don't think. Equally, I know that you and I have talked. I have very much the same, shared concerns.

I'm concerned about any sort of category or bucket that we put ourselves into beyond type one/type two as being forced down the various registry throat by the GAC and others. I'm very concerned that it's going to be against us. I do also want to make sure that we are getting credit for our mitigation.

On the other hand, I want to think and challenge this idea. Something you said made me think, "is this really how it has to be?" I would love to get some more group discussion around it. You said – and I heard you say – that we want to make sure that the registries' mitigation efforts are being captured in DAAR. I'm going to push back on that for a minute. Do we – must we – capture our mitigation in DAAR? If ICANN has said again, and again, and again, and we wanted to help them say ... And we can go back to that work that we had done, that continue to say that.

But if the goal is that ICANN says, "DAAR is just a tool and it's just data." It's not the end of the process. It is a starting point. It is some information about what's going on in the DNS. It's a snapshot, right? Let's say that we

---

make that tool, that snapshot, a little more meaningful. Then, it's up to us, individually, within our own companies and within our own organizations, to advertise our mitigation. We can do that through advertisements on our sites. We can put statistics up if that's our bent. Every single one of us approaches this a little bit differently.

And to be able to say, "This is what we're comfortable with. This is the publicity." Some registries are comfortable open-book, "Here's everything we do. Here are all of the things we've taken down. Here's every single number." Other registries want to keep that close to the vest. They want to present a more composite picture. Rather than assuming that one size fits all and shoving it into DAAR, what if we talked about how to make the DAAR data meaningful in such a way that it then points back to the different registries' efforts?

And if some registries are having zero effort, maybe that's telling in and of themselves. Not that, necessarily, ICANN could act on it, but we don't want ICANN to act on DAAR anyway. Ultimately, at the end of the day, if we don't include mitigation in DAAR, I feel like we may be closing the door to allowing compliance to use DAAR. I would love to have people poke holes in that because this is literally speaking off the top of my head, reacting to what I heard you say.

I would love to hear what other people think about that idea and if that really moves the ball forward with this DAAR project or doesn't move the ball forward. I'm going to go on mute for a while, now. Thanks.

---

JAMES GALVIN:

Thanks, Kristine. Excellent question. Before I respond, does anybody want to jump in and offer comment? Let's see. JC put something in the chatroom, here, talking about "the problem is that many people, meaning the other side, just stop at the snapshot. Making DAAR more comprehensive avoids the issue for most of us." Actually, thank you, JC. That, in fact, would be part of my response to Kristine. I don't think it sets the question aside but that really is my only real response to why we wouldn't put it in. It just leaves it all to each of us to have to deal with it.

My concern and my response in this to you, Kristine, is, I guess, maybe I'll just expand a little bit on the way I've said this before. The problem is that the industry is painted a certain way based on what's in DAAR. I guess that in order to be able to say we don't need to represent our mitigation at all in DAAR, what would make me personally comfortable in that is if the DAAR data, as presented, actually had a messaging in such a way that it got rid of this broad-brushstroke of "systemic problem." If there was a way to make that particular message go away then I would absolutely come away from the position of wanting to have mitigation be there.

I'm really after that particular piece of things. I do think that you have a good point there. If we don't do that then this becomes a little bit visible to compliance. Does it become data, then, that compliance can use? We do have to assume that somewhere down the road compliance is going to be able to make use of DAAR, even though the claim is that they officially don't do that today. JC, you have your hand up. Go ahead, please.

---

JEAN-CHRISTOPHE VIGNES: Just briefly. Thanks, Jim. I agree with what you said. I think our whole exercise for weeks and months is a perception problem. We can all lament it. I know I do. I know I agree with Kristine in principle that we should not have to do that and we should not impose a new way for TLDs to express what they are doing to fight abuse, in an ideal world.

The problem is that we do because of the brushstrokes that you just mentioned. And so, saying, "Let's have DAAR evolve and then we can have, individually, on top of it," I appreciate the sentiment but I think it doesn't go far enough, considering what the other side of the community has been saying for months, now.

I'm not advocating for each and every one of us to actually have an open door policy and say, "Hey, look at what I'm doing to fight abuse!" What we have on the spreadsheet, I think, is a very strong first step. But I don't think it's enough and I don't think it should be less than that. That's what I wanted to say.

JAMES GALVIN: Thank you, JC. I appreciate that. Rick, you have your hand up. Go ahead, please.

RICK WILHELM: Thanks, Jim. As it relates to including mitigation in the DAAR report, I would just offer that a lot of people likely would be against, or at least ambivalent about, recording or disclosing their mitigation efforts publicly because, frequently in these kinds of efforts, disclosing mitigation efforts can undermine their future effectiveness. Thank you.

JAMES GALVIN: I'm wondering if you could say a little more about that. I get the ambivalence issue. People can often be ambivalent about lots of things. But could you say a little more about how it undermines future mitigation efforts, please?

RICK WILHELM: Yeah, sure. I could probably word that a little bit more strongly. It might not be ambivalent. It actually might object to it. Because if you have an effort that you use to mitigate DNS abuse and it's disclosed, then your adversaries, those that are abusing the DNS, can adjust their tactics and methods to help avoid or reduce the effectiveness of your countermeasures. They can evolve their techniques because they might not necessarily know what you did or that you even found them.

Sometimes, in this sort of an effort, as you well know, Jim, from your experience, adversaries don't know if you thwarted them or if their techniques just didn't happen to work because they were ineffective. Thank you.

JAMES GALVIN: Right. Thank you, Rick. JC, I don't know if that's an old hand or a new hand. Let me just clarify one other thing then, Rick. I agree with you, actually. That, I understand. You're absolutely right. In fact, I didn't say it earlier but that contributes directly to why not taking type two and trying to create groupings around mitigation methods is actually kind of important.

---

Again, it's not public information. Creating those groupings around it means that somehow we have to expose that, and that would not be something that we would want to do. You've just highlighted an excellent, specific reason as to why that would also be a bad idea.

What I was suggesting in representing mitigation to be put into DAAR, what I meant by that is not the method of mitigation, not the mitigation action itself, just the fact that mitigation occurred. In some way, just indicating the fact. The example that I have in my mind is the Anti-Phishing Working Group. When they do their semi-annual report about the presence of phishing in TLDs and they do their rankings and they publish their data, one of the things they've added the last couple of years is the uptime of the domain that is phishing.

The goal here, of course, is to have a shrinking uptime. So they demonstrate, based on the data that they look at, that names come into existence, they start phishing, and they actually record, track, and calculate the average amount of time the domain names stay up when they've been identified as abusive.

And so, the fact that you took action is visible because now you have this metric. You have this uptime metric associated with your TLD. The smaller the number, the better. What I would be looking for is some kind of metric like that. Some kind of way to indicate that the domain names from month to month ... You know, you might have 10,000 abusive domain names every month and that's just constant, and that's what it is in your TLD.

---

Well, that doesn't mean that your TLD is particularly abusive. If it's a different set of 10,000 names every month you should get acknowledged for the fact that it's a different set of names. What's the variability in the names? Can you average the change and the churn in the names that are flagged as abusive, create some kind of metric, and make that visible? Maybe it's something that we tell ICANN or maybe it's just something that they have to do a greater analysis of the data that they have.

I don't know if there's an action on us to do some reporting, but that's what I'm looking for, not the specifics of our mitigation. Just some way to get acknowledged for the fact that we don't have control over abuse. The best that we can do is be reactive to it: "Oh, by the way, we're actually pretty reactive and we're on top of things." There should be rankings that show that.

Okay. I'm not seeing any other hands. JC is just giving a vote of support to the point that you made there, Rick, and what I was expanding on a bit, in the chat. Okay. If there isn't, really, anything else to say about it at the moment, I don't really have anything else of substance to talk about today. We'll take the action to send the spreadsheet to Samaneh and John and ask them when they'll be ready to meet with us again.

Maybe a related action here, Kristine, is that we should take some of this discussion and presentation, here. Maybe we need to try to create some black and white suggestions and words here, out of this, and kind of document so that people have a better opportunity to look at it and really think about it. It'll also broaden our ability to get more of the community in on it because we can send it to the mailing list. Maybe we'll get some

---

additional discussion out of some others than just those who were on the discussion, here.

I think, with that, I'll do just a quick call here before we jump to talking about ICANN67. Any other comments or questions of substance, here? I'm more inclined to give people time back in their day if we don't have any place else to go right now.

Let's jump to Sue's last item here about ICANN67 planning. I can see that you had a note there for us to tell everyone that we have a meeting slot for ourselves. It's a 90-minute meeting slot on Monday from 13:30-15:00, local time. Thank you, Sue. She's putting up the entire schedule for us to look at it. We can see what it's competing with. For those of you with better eyes than me, maybe, Sue, I'll let you speak to what else is on the calendar, there.

SUE SCHULER:

Sure. We're up against the RPM PDP, the RrSG has a DNS abuse meeting at the same time, the NCUC members' meeting, and the BC ExCom. We actually don't have a lot that we're competing with. My biggest thing that I need to walk away with here is, are you inviting John and Samaneh to this meeting so that I can get that in their calendar, as well?

JAMES GALVIN:

Yeah. To be honest, I think my immediate reaction is that I'm not opposed to having them come along to the meeting if we have something to talk about with them and that's a little hard to predict right now. Maybe, if

---

they're willing, it would be good to highlight the meeting slot with them and just have them reserve it and block it out with just that caveat.

As we're beginning to run experiments with them it's going to depend on whether there's something that they're going to have to present to us and we just don't know that yet. I don't imagine we'll know the answer to that question for probably several more weeks. We should keep the opportunity open, I would think, but we can't make a commitment, yet. Is that fair?

SUE SCHULER:

Okay. Yeah. I will ask them to block it off and play it by ear that, hopefully, we'll have something to discuss with them.

JAMES GALVIN:

Right. I mean, Rick is saying that the data slicing should be done by then. I agree with you, Rick, especially this particular data slice request. I hope it's done within just a couple of weeks. Maybe three, at most. But I'm also expecting that we're going to continue to give them data slice suggestions to look at and we'll need to schedule reviews of that data. I don't know if that will fall on an ICANN meeting or fall on a meeting outside of that slot.

That's what I'm leaving the door open for, that's all. If there's a slice that they're working on and they have it, then great. If not, even for ourselves we won't know for sure what we're going to do with that meeting slot for another few weeks yet. JC, you have your hand up. You get the last word unless another hand goes up.

JEAN-CHRISTOPHE VIGNES: Yeah, sorry. At the risk of being rude, the ICANN meeting is a month from now. We have four meetings to do beforehand. We know how busy the ICANN staff is. I would honestly prefer to invite them now and then realize that we have to postpone than realize at the last meeting that we would be in shape to talk to them and not have the opportunity. In other words, ask for forgiveness instead of ... The other part of the saying. We got quite a bit done at the face-to-face meeting in Montréal so I don't think we should waste the opportunity for Cancún. My two cents.

JAMES GALVIN: Thank you, JC. Yeah. You said it somewhat more directly than what I said. I think that's really what I was suggesting. Let's send them a note, invite them, tell them to please block out that time. But in all fairness to them, just recognize that we were hopeful, too, that we will have a specific agenda item to discuss with them at the time. As long as we have it then, yes, we will meet. If we don't then the worst case is that we might ask them not to come and we'll use the time ourselves. So, just letting them know that we might cancel at the last minute if we don't pull an agenda item together, that's all.

Let me look at the one last comment here in the chatroom while I wait for any other hands for any other business. Owen: "Are we anticipating an open or closed meeting at ICANN for this discussion?" I would say that the meeting is closed just to registry operators, just ourselves and the stakeholder group, because it really is just for us at the moment. I mean,

---

even our weekly meetings are just for us, I would think. But I'm open for suggestions. That's my initial idea.

Sue is just telling us that she requested a closed meeting. I imagine we could change that if we want.

KRISTINE DORRAIN: I think it should be closed. Thanks.

JAMES GALVIN: Yeah. Is there anyone who disagrees with it being closed? Kurt is saying that he does think that's the correct approach. I mean, it's a good question to ask. We should always deliberately make a choice about that kind of thing. I'm seeing a plus one, here. Two plus-ones. We've got Rick and JC. Okay. We'll stick with closed. That's what we've done before and we'll continue that way. Dietmar is on there now saying, too, plus-one. Thanks for that. Okay. With that, one last call for any other business? JC, I'm assuming that's an old hand. Let me just say thank you to everyone and we'll see you next week.

SUE SCHULER: Julie, we can end the recording.

**[END OF TRANSCRIPTION]**