
ICANN86 Seville | PF – Joint Session: ALAC and SSAC
Tuesday, June 09, 2026 – 14:45 to 16:00 CEST

KATHY SCHNITT

Hello and welcome to the joint session between the SSAC and the ALAC. My name is Kathy and I'm the Participation Manager for this session. Please be advised that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Interpretation for this session will include English, French, and Spanish.

During the session, questions or comments will only be read aloud if submitted within the Q&A pod. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record, the language you will speak if speaking a language other than English, and speak at a reasonable pace. With that, I'm happy to hand the floor over to Jonathan Zuck, ALAC Chair, and Ram Mohan, SSAC Chair.

JONATHAN ZUCK

Thanks a lot and thanks, everyone, for being here. I'm sorry I am MIA today. I'm a little under the weather, but wanted to join this call because it's such an important meeting for us, every ICANN meeting, to get together with SSAC and find out what you've been

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.

working on and look for opportunities for us to work together to get the word out on some of the work you've been doing and widen the audience for those efforts. So thanks and welcome, and Ram, I hand it to you.

RAM MOHAN

Buenas tardes. Good to be here. And Jonathan, sorry that you're not feeling well, but hope you're on the path to recovery. Thanks for coming in. Look, from the SSAC's point of view, this is an important meeting because we look to you and the ALAC as a very important part of the community, who much of what the work we do is eventually aimed at.

We write many reports, many of them are aimed at board members and other parts of the community. But at the end of the day, the things that we are providing advice on and providing suggestions on eventually translate to the users of the internet. And you have a distribution model, if you will, that can disseminate the information that we are providing. You have a way between the ALSs and the various groups that constitute the ALAC. We really look forward to finding ways to amplifying what you're doing and providing you with content, providing you with information, and in some rare cases, with advice on things that you can do. So therefore, that makes the ALAC and SSAC conversation at each ICANN meeting an important one.

I will say that just as kind of opening comments, one of the things that we really want to do and want to open a conversation with you

in a very candid and kind of collegial way is we're not satisfied with where this relationship is. That's not because it's not doing well, but because we want to go a level up, right? We think there are things that we can do even more, and we want to explore that with you, and we want to figure out what some of those things might be.

Now, one of the things that, and you've seen several SSAC colleagues here, one of the things that when we discuss SSAC and its engagement in the community, one of the things that we always focus on is that we stay within the areas where we have competence, and we work in those areas where we have competence.

So we're good at looking at topics that relate to security, stability, resilience. We're good at thinking through what some consequences might be and postulating several things that the community should be thinking of. But what we're not specialists at is how to go and have that message reach the end user, how to have that message go and actually have an impact. That's one of the big reasons why we are quite keen on engaging with the ALAC, because we think you have the ability, but we want to get more organized with you.

I'll confess from my side that the inter-sessional interactions between the SSAC and the ALAC are not where they should be. Most of our interactions happen at the ICANN meetings or in the margins of the ICANN meetings, in the preparation for the ICANN meetings, etc. But if I look at how do you upgrade, how do you go

to 2.0 of this already fruitful engagement, I think we ought to think about how do we make the inter-sessional conversations happen, and what are some joint outcomes that we want to achieve.

What I'd like to challenge all of you here in the ALAC with in a conversation with us is what does good look like? Because we're already successful, so we don't need to go and define success in the sense of we're meeting and we're conversing and sharing information with you, things like that. But I think we ought to have a pretty candid discussion of what does good look like and how do we get there.

I'll leave you with that as opening comments and give it back to you, Jonathan, for anything else you want to say before we go to our planned agenda.

JONATHAN ZUCK

Well, shucks, Ram. I feel like we're having a restatement of vows or something like that, so it's very exciting. It's easy for us to take each other for granted and to recommit to each other here years into our relationship like this and restate our vows, I think, is a very powerful thing, so I'm with you 100%.

We have made many promises to communicate more intersessionally that we have jointly broken, but I think you're absolutely right to press the issue, and I think we would like to do that as well. Part of the challenge for us is that we're working out our own expertise in the area of getting messages broadcast out to

a broader community and things like this. It's been a disjointed history and we're trying to figure out how to systematize that better.

In fact, that's the central theme of our upcoming ATLAS, where we'll actually have some of our ALSs and more active individual members joining us in a larger meeting at Lisbon. All of this is very pertinent and I think good time for this conversation, because I think we share the same goals and let's find that path forward and redouble our efforts there. I certainly agree. I see a little bit of a queue forming, so I'll go ahead and call on Robert. Go ahead, please.

ROBERT GUERRA

I'll make my comments in Spanish. First of all, I would like to thank ALAC for having this meeting with SSAC, Roberto Guerra, member of SSAC. What Ram mentioned is on point. What we want to do is improve our conversation or discussions with the security experts, which is the SSAC committee and those of you that are in constant contact with the users. And even more important is this because the changes are more rapid and the safety topics are more important. And so it's good for us to have this discussion within our meetings.

But I would also like to add that in SSAC, we not only speak English, as you can see, I also speak Spanish. We have members that speak French and Arabic. So we are aware that there are different languages and we want to see how we can collaborate with you.

And that would be a pleasure for us to be able to do this. And so I await the presentation that Ram will be giving.

RAM MOHAN

Thank you. Matias, go ahead.

MATTHIAS HUDOBNIK

Hello, everyone. Can you hear me well?

RAM MOHAN

You can speak up a little.

MATTHIAS HUDOBNIK

Okay, perfect. Now better? I hope it's better. I would like also to come in quickly. First of all, thanks a lot for you both to start the session and also for your points, Ram. Since I'm also liaising between the two communities, I think from my perspective, or at least I would like to share a bit also my personal view, I think there is always some space to, let's say, to be better from my perspective.

I'm also very happy to, let's say, try to change things where we can, also from the SSAC perspective or ALAC as well, since I'm also trying to distribute all the time the kind of reports. I did it since the beginning. Yeah, I mean, there are some of them, I think, I mean, people are definitely engaging with it. Some of them, I'm not sure, but it's maybe also due to the fact that they are quite technical.

I think here, again, I definitely seconded what you said, Ram, so maybe we could get more input also from that large community, which I know very well and which is also very on my heart, to make it even more efficient. I think that would be good, where also people say, this is something where we could improve things. And also with, I mean, we will come later to the cyber safe campaign. I think, yeah, we are discussing this for a long time already. Thanks.

JONATHAN ZUCK

Bardzo dobrze, Matthias. And Alan, you go ahead next.

ALAN GREENBERG

Thank you very much. One of the problems ALAC has had forever is how to deal with ALSs. We have ALSs, if you look at the bylaws, because they have people on the ground, but we've always had a problem actually getting to communicate to the members within the ALSs. We've never had a good mechanism for it.

And we're just about to launch something that we hope will work. And it dawns on me, based on what Ram was saying, we could use that same mechanism, not only to get our message out and trying to recruit at large workers, but get messages from the SSAC that you want to distribute on the ground, or get information back from people on the ground. And we could use that same path. So that sounds like a very cooperative thing that we could essentially double the effectiveness of the communication path once we get it working.

JONATHAN ZUCK

Yeah, it's what we're calling the At-Large loop. And we've been fussing with it. And the first thing was the Safer Cyber campaign. And our mate is next in the queue, but we've started some pilot projects with the phishing courses that have begun to be taught. So we're getting the rust out of the communications pathways. And so I think the timing of this is good. Amrita, go ahead, please.

AMRITA CHOUDHURY

Thank you, Jonathan. Amrita, for the record. And you stole a bit of what I was going to speak. Yes, there could be more collaboration. No, that's okay. I'll just add on that. We could have definitely more collaboration. And the community wants more collaboration, I would say.

As Jonathan mentioned, we have started the pilot of the phishing campaign. We have people in the room who have been doing it in the community. It's not grown to that extent, but people are doing in APAC, in Africa, and other places, people have started doing the phishing campaign. It took a long time to come in, because our production cycle was a lot longer. If we are looking at community engagement at the issues in the safer cyber campaign, etc., if we can have modules prepared, which we can help our community reach out to the others in the ecosystem, that would be really helpful. If we really want effect, those are the things we should collaborate.

Perhaps SSAC people are more techies than us. They can help us in even creating those modules much more faster, which we can percolate it. Currently, we're trying to create a toolkit, give everything, so that it's easier for everyone to do. So, that, I think, is one thing where we can be more effective as partners. As you said, we have the reach. Not everyone can do it, but there are many who want to do it. And the ecosystem needs those safer cyber campaigns, I would say.

RAM MOHAN

Let me just briefly comment on that. And I'd invite SSAC members here to also opine. I think it's well within the capabilities of several SSAC members to design something like that in collaboration with you, because relatively speaking, I would imagine it's a much lighter lift. You know, we have members who are professors and who design much more heavy-duty courses, if you will. So, something like this is likely to be not only something they're familiar with doing, but also would be aimed at the level that that calibrates for the level that you need it to be at.

So, if that's interesting, then then I would put it this way. It's on you to come to us and say, we want to do this. Can we do this together? Because it's not going to be, I mean, the SSAC is busy with other stuff. It's not going to be really possible for us to remember it and then come back and say, hey, we talked about it at that time. Do you still need help? Right? So, if the ALAC thinks that this is important and useful and valuable, we're available. You know, we

are the resources you can call upon. We are available for that. But just to be clear, the ownership has to be with you on that. And we will be willing and able partners on that. But it's got to originate with you because you know your audience better than we know them.

JONATHAN ZUCK

Yeah, I think we're on the same page there. Like I said, we're in process of kicking off our own training wheels on this very issue. So, I mean, I think the timing is good for this. Maciek, please go ahead.

MACIEK PIASECKI

Maciek Piasecki here. I'm actually one of the EURALO leads for the phishing campaign. And that was one of the questions I had prepared. I'm not sure if this should be discussed here, but we do have the slide deck and the resources that the outreach team at ALAC has prepared for us. And they're very good, but they're in a bit more of a traditional phishing campaign.

And I would love to know what are the future threats that we should be making people aware of, especially that the purpose of this campaign is to be training future trainers. So, making sure that they are not teaching about the threats that might disappear in a couple of months and be replaced with something else would be some amazing portion of knowledge we could get from you. So, we can either discuss it here, but it's going to take time. Or maybe if

you say we should come to you, who would be the contact point we should reach as the training leads?

RAM MOHAN

Thank you. Just very briefly on the contact point, it would be to me with the SSAC staff. And we have SSAC staff here. It would be a combination of those. And our staff are brilliant at figuring out who to then go and task to get the job done.

JONATHAN ZUCK

Yeah, definitely. And I think that's part of why we were doing this session, is looking at some of the things that are coming on the horizon that we want to potentially explore as in-user outreach topics. Pari, I hear you have your hand up in the room. Please go ahead.

PARI ESFANDIARI

Thank you. In terms of collaboration, I think ALAC and RALOs have roles. One is reaching to the end users. So, in that sense, a couple of people already spoken. But we are also policy people. So, we want to better understand threats that are emerging. I think that area also, we need your help.

What is in horizon? What is coming? Yesterday, we had a session on AI and you saw how popular it was. So, it is very important for us as policy people to understand what is coming, not what is right now people are seeing and feeling and dealing with, but also what is in the horizon from the end user perspective. Because these

issues are discussed, but from different perspectives. So, help us to better understand those. Thank you.

RAM MOHAN

All right. Thank you so much. That's so relevant. And we do have a slide later on to go through that and to give you some examples of what we're doing in other parts of the community that perhaps might be informative for what we want to do here together. So, hold the thought and come back in when we get to that point of it. SSAC members, anyone who has a perspective would like to join in?

JONATHAN ZUCK

Or we can move forward into the substance.

RAM MOHAN

Nabil, please.

NABIL BENAMAR

Thank you, Ram. This is Nabil from SSAC. So, I'd like to jump in the discussion about you can reach out to us. We have expertise in the field definitely and we are willing to help in this campaign, phishing campaign, and also raise awareness about the role of AI now in cybersecurity threats and advocating for something that can be done and tailor it for the end user in a proper way, proper language that can be understood and compiled by anyone. So, we are really happy to help in this. Thanks.

JONATHAN ZUCK

That's excellent.

RAM MOHAN

All right, Jonathan. I think we're off to a fast start on beginning the conversation. And I'm imagining, Jonathan, that when we get to the safer cyber piece of it, we'll have maybe we can not talk only about safer cyber, but also about the broader engagement and how do we make this a fruitful thing that sustains over time, right?

I don't see any other hands in the room here, Jonathan. So, shall we go on to the next part of the agenda?

JONATHAN ZUCK

Let's do it.

RAM MOHAN

Okay. Next slide, please. I wanted to just share with you in the ALAC what the SSAC -- Oh, so sorry. I missed your hand. Please.

EUNICE ALEJANDRA PÉREZ
COELLO

Thank you. Eunice, for the record. In my perspective, one thing I think constantly I have the opportunity to assist to the meetings or the sessions that you present work-wise. And I'm very interested in the meetings and the session with ALAC. I only see maybe present one topic or talking about one topic only. And then this topic you'll present in another session.

So, I would like, as Pari said, that it's very important to identify, to us identify, no, sorry. Could you identify us as end users who maybe, as you say, you comment, we have maybe more skills, technical skills, and other not. But his work in Pari, the people understand. And I understand that. And I think that other persons who don't have maybe the same skills understand that. And maybe if you bring that experience or expertise of bringing to all of us, we are understand that. I'm not sure if I, but I can speak in English and Spanish.

RAM MOHAN

If you'd like to speak in Spanish, please feel free to. It's up to you.

EUNICE ALEJANDRA PÉREZ
COELLO

If you understand, Ram, understand that I tried to say.

RAM MOHAN

Let me just paraphrase what I thought I heard. What you're saying is that certainly within the ALAC, there are people who have a technical background and an understanding and may be able to contribute to the work that the SSAC does in several of its work parties. And the question underlying this is, what is the mechanism to bring that kind of talent or expertise inside of the work parties that we do? Did I get the question correctly?

EUNICE ALEJANDRA PÉREZ COELLO No, how to bring care to ALAC. I think sometimes, sorry for the word, I think we don't know any technical skills. And sometimes talking with a basic knowledge about the security and substance, I think, or skills. And in the meetings that you have in the session that you present in his work parties are more technicians. But I don't know. I understand that. And older people that don't have the same skills of technician skills understand that.

RAM MOHAN Got it. Understood. So this is a good question. And the SSAC itself is in the midst of evolving on this, right? Because at the ICANN meetings, the SSAC for the last couple of years now, we are open by default. So with a few exceptions, all our meetings at the ICANN meetings are open. It used to be that we had all our meetings closed. But one of the things that we're trying to figure out is how do we run a work party meeting, right? Which is kind of intentionally aimed at SSAC members engagement and do the work. How do we do that at these ICANN meetings and at the same time recognize that there are other members of the community who are at least observing and watching?

And in Mumbai for the ICANN85 meeting, for example, there was one work party where if you'd come and watch the work party meeting, you might have been bored out of your mind. Because in the one hour that we were there, we worked on one segment of the document that we were working on. And we had members going

back and forth on what does this word mean and how should that be changed, right?

So we thought that is not useful. So at this meeting, for instance, we've been doing a little something a little different. We just had earlier in the day a work party meeting, our AI and DNS abuse work party. And what we did there was we summarized the main areas of engagement and we invited SSAC members to speak to it. And we're trying it out for this time, but we had a rule that observers are there only to observe. They don't get to engage, participate, provide commentary, right? So that's what we're trying out.

Now, when we have a document done and complete, we work very hard to come to you and to present the findings of our document to speak to that. We have Greg Aaron here. He had presented on DNS blocking. Martin Artson, I don't know if he's here, but he had presented on open source software and how the DNS depends upon that. So we've had several. When we have a finished work product, we come here and we present that.

And those ones, we try very hard not to keep it at a very high technical level. We try and get that to the level that is digestible and understandable by everybody in the community, right? But we ourselves are experimenting with how do we both stay open and at the same time, stay productive for our members. That's the tension for us. Thank you for that question, though. Maciek, you're back in the queue.

MACIEK PIASECKI

To follow up a bit to what you said, we do have varying levels of knowledge in the community and we've got different specializations. So I could probably tell you more about GDPR than you know, and you can tell me more about the DNS than I know. So what I was thinking, what you inspired me to maybe we should present you with the list of topics that we would find very relevant to the current discussions in ICANN that we don't know so much about as ALAC. And maybe this could also inspire you to make some sessions that could be also interesting to the wider community past the ALAC.

RAM MOHAN

I love that. And I can tell you ahead of time that our list of things we don't know will probably be much bigger than the list of things you can give us because we know a lot about a few things and we've worked pretty hard to be pretty deep in that. But especially on a lot of policy oriented things or legal oriented things, the SSAC doesn't pay a lot of attention. So I love that idea of you presenting a list to us and then we can come back and work on it.

MACIEK PIASECKI

This could be a nice approach so you could do a list for us and we'll find the experts.

RAM MOHAN

Okay, lovely. Great.

JONATHAN ZUCK

That's the next in the agenda is to go through some of the things that you're working on.

RAM MOHAN

That's exactly right. And so I wanted to share what are some of the things that the SSAC is currently engaged in and working on. And we actually have the advantage of having several of the work party chairs here to be able to speak to that. I won't read everything on the screen. Let's go to the next slide. And I'll hand it to you, Rick.

RICK WILHELM

Very good. Thank you, Ram. Rick Wilhelm here for the RIDE working group. RIDE is an acronym for the title that you can see at the top of the slide. And you can read our goal over there on the left. We're working on this these days because it's become increasingly clear that integration with the DNS and domain names into new technologies is going to present some new challenges that may be impacting the stability and security of the DNS. And so what we want to do is work on getting some advice out there for folks to work on proactively addressing those issues in order to help maintain user trust and hopefully be addressing issues in advance to try and work on preventing the possibility for additional abuse.

There's some related work that's going on over in the ITF that some folks might be aware of. This is not competitive to that work. It's complementary to that work, just in case you're wondering. As with all of this stuff, this is the primary audience for here is the ICANN community. Most importantly, accredited registries and registrars and people that are working on applications that would be developers working on applications that would integrate domain names into their applications. And, of course, people in the broader ICANN community.

You can see our key areas of study over there on the right of the list. Probably primarily among those is the domain name lifecycle because changes in the domain name lifecycle and maintaining updates that if you're doing an integration, you have to stay in sync with those because, as I've said in previous meetings like this, otherwise it will likely end in tears. The bumper sticker down there in the lower left, coordinating with the ICANN TSG, that's a new technical study group that's in the process of being spun up.

That's something that ICANN is starting on related topics. That's something that we'll be coordinating with once they get operational. We're expecting a blog post on that from ICANN org any day now. It may have come out today. I don't really know. I didn't look, but probably not. Otherwise, Ram would be saying right now it has come out today. So, if Ram says it hasn't come out, then it hasn't come out. That's about all I've got, and I assume we'll take questions at the end. Thanks. On to the next slide.

RAM MOHAN

Questions for Rick before you go to the next slide?

JONATHAN ZUCK

Yeah, this is Jonathan. This is a perfect example. I mean, this is something I actually raised as a possible plenary topic for ICANN, but we weren't sure when the right time was for this conversation because I think there's going to be both technical and cultural shifts ahead in the new round because of the new technologies and blockchain-based domains and things like that and how that integration is going to take place.

So, this is something where it's a two-sided thing. There may be policy-related issues, as Pari raised, because we have in the past amplified SSAC work into the policy arena to make sure that your research got acted upon in a couple of different instances, and this may be one of those areas where we can be an amplification of your voice within the ICANN community. But determining what, if anything, is a message that needs to get out to ordinary end users, for lack of a better term, would be one of the challenges in this particular case, or if this really is just a policy issue to prevent confusion on their behalf.

RICK WILHELM

Thanks, Jonathan. At present, the findings don't contemplate raising anything related to policy issues. This is for how to be operating inside the realm of existing policy. Thanks.

RAM MOHAN

No other questions in the room. So, let's go to the next slide. This is DNSSEC operational considerations. Chaoyi is not here in the room. Oh, you're here. I haven't even said hello to you. Hi. So, Chaoyi is here. So, he is the co-chair. So, please.

CHAOYI LU

Okay. Thanks, Ram. Thank you for not noticing me. So, my name is Chaoyi Lu, and this work party is called DNSSEC operational considerations. Ram and I are the co-chairs of this one.

So, DNSSEC, we know, has been there for long, and the full function of it requires collaborative efforts from registries, registrars, resolvers, and also domain registrants and our end users. So, historically, there have been impressions, some impressions, about DNSSEC operational complexities and even challenges, and we are seeing a lot of opinions and measurements from different angles and point of view.

So, with this in mind, this work party was established to provide a practical guide to strengthening DNS security. So, we do this by gathering and summarizing DNSSEC facts and DNSSEC data in order to demystify this protocol for our audience and make it easier for internet operators to adopt safely.

So, some questions we try to address includes, what are the unique security value and functional elements you should know about DNSSEC? What are the pros, cons, or even lessons learned under

different scenarios? How has tooling and automation developed for more seamless deployment? And finally, what are the major technical or non-technical determinants if we are pursuing a broader adoption?

So, we are working towards publishing our report before the next ICANN meeting. So, please stay tuned if you want to know more about operating DNSSEC, and hopefully, you'll consider deploying on your domain. Thank you.

ALAN GREENBERG

Questions for Chaoyi.

RAM MOHAN

All right. Let's go to the next one. AI's impact on DNS, SSR, and abuse. Matthias and Laurin are the co-chairs and both present. So, who wants to go? Go.

LAURIN WEISSINGER

Matthias, you're not saying anything. So, I assume I'll go. So, I'm Laurin.

MATTHIAS HUDOBNIK

Yeah, you can start if you want. Otherwise, I can also, but I thought if you were there, it's maybe better, but I'm also happy. But please go.

LAURIN WEISSINGER

Awesome. Thank you. So, I'm Laurin. I'm one of the two co-chairs of this one. So, we're currently in the outline stage for our work on AI. We're really deep into discussions around how do we scope this? What are we looking at? We had a work session today. Unfortunately, if you're interested and you learn about this now, it's too late to come to that work session. Apologies for that.

So, essentially, our scope of work is to kind of look at offensive and defensive uses of AI as it relates to the DNS and the DNS ecosystem. We are aware this is a time-sensitive topic. So, a lot of our discussions actually are about how do we scope this in a way that we can complete the work quickly enough so that you all get an output while at the same time staying serious and covering what is needed.

And our goal is really to first come out with a short educational report that's helping us as a community to better understand what's going on and then move from there. So, it's very likely that this will be with us as a topic for quite a while. So, we're trying to be quick and establish something, and then we'll see how to move forward.

RAM MOHAN

Questions for Lauren or Matthias? Okay, do not see any. Let's go to the next slide. DNS transparency, Raffaele and Gautam.

RAFFAELE SOMMESE

Yeah, thanks. So, this is actually a pretty newborn work party, and the idea stems actually from research that me and Gautam has done in the past of the fact that the current mechanism for publishing zone data has limited visibility in certain intraday events, and there is opacity, basically, in the fact that zone files are published once a day, for example, in the CZDS ecosystem, and this opacity impedes the detection and the mitigation of malicious activities.

So, the goal of this work part is really to evaluate mechanisms for sharing near real-time zone data to bridge, basically, the security gap, and the motivation is to try to provide malicious activities that spawn from DNS abuse, but also domain ejecting that was a good chunk of the research that Gautam did in the past, but also the linkage between certificate ecosystem and the domain ecosystem.

So, we would like to try to do this by answering four questions in this work party, that basically is why we need this transparency and what events we want to record from registry and registrars in this log of changes that happens inside the DNS ecosystem, how we get and store these events, and who can get access to this data and for which purposes and with which mechanism.

So, this is more or less the general idea that we want to pursue. We are at the initial stage. Tomorrow we'll have the session for the work party, so if you want to join and you're curious about the process that we are following, please do.

RAM MOHAN

Questions?

JONATHAN ZUCK

Ram, this is Jonathan again. I feel like I'm going to have, this is a general question, but want to ask it along the way, is that as we go through each of these work parties, are there things in which you see opportunities for partnership that we should be hanging our hat on in terms of, it's good for us to be informed for sure, and we appreciate that, and certainly when things have policy implications, we can help with that.

But as we talk about sort of magnifying or amplifying these messages outside the ICANN community, perhaps making part of your presentation what the vector is for end-user awareness or end-user interest that could be better supported, then we can begin to think in terms of how to expand our activities, if that makes sense.

RAM MOHAN

Thanks, Jonathan. That's a really good point. And Danielle, if you could just make that as a note for our future conversations to kind of come into this with the lens of not only just sharing what we're doing, but perhaps also identifying threads that we can pull on that we can engage with and interact with.

Responding on the fly to your question, though, of these four topics that are here, to me it sounds like the two that may have relevance

and kind of a good audience perhaps are the responsible integration into the DNS ecosystem topic, which, Jonathan, I like your kind of the thinking that you have that maybe that's a good topic to propose for a plenary session to speak about what it is, but also what some of the policy implications might be, user implications might be, etc. So, that perhaps is something. But even without the plenary, to me it feels like that's a topic that is quite ripe for engagement and amplification.

The second one, which is, we're still in early stages, and Laurin and Matthias can speak to that, but if you look if you go back a slide to the AI impact slide, you look at what we say, we're saying it's a short educational reference report, right? So, that's a report intended to inform and to kind of level set. And to me that's, I think, a fairly straightforward thing to come and bring in front of the RALOs and the ALSs, etc. So, to me that's a second topic that feels directly relevant.

The DNS transparency and the DNSSEC operational considerations topic are, I would say, relatively speaking, more inside baseball. They're kind of aimed at a more, perhaps a bit more technical audience or a more specialist audience in there. So, that may be a later discussion or an overall information item rather than something to specifically talk about. Amrita, you have your card raised.

AMRITA CHOUDHURY

Yes. Thank you, Ram. The DNSSEC, for some, at least in the APAC community, they have a big appetite for it because we have, though we represent the end user interest, but we also have a lot of technical capability which is built, say, for example, in the Pacific Islands or anywhere in India or even Nepal or any places. They have a huge appetite because our ALSs just do not represent the end user interest. They also work in the community to build capacity. So, we've seen the DNSSEC courses do well in certain places. So, personally, I would not erode it. That is also very beneficial.

RAM MOHAN

I really like that perspective that you're providing because what Chaoyi is leading up is, I think, eventually is going to be a pretty solid reference document that doesn't pull any punches. It's not a cheerleading only or a doomsday only type of a document. We're looking to talk specifically about if you want to deploy DNSSEC, what do you need? How do you build? You know, what is the capacity? What are the pieces to it? So, that may well be something that we can take on the road with you. And the road these days is mostly virtual, but you can still do that.

All right. I think we are done with that piece of the four work parties that we're working on. And, Claire, you said there is a host of hands here in the room. So, let's go to Jonathan. You want to manage this?

JONATHAN ZUCK

Sure. Maciek.

MACIEK PIASECKI

Maciek Piasecki, EURALO. I feel called out on the topic of transparency because it's not exactly related to what you've been presenting, but during the DNS abuse PDP, part of the discussion is how transparent the procedures for initiating the associated domain check should be. Should they be disclosed to the public or should they be kept as internal documents? The argument for keeping them secret is that making them open would help cyber criminals to learn from them and circumvent it.

And so, well, from my perspective, someone who's helping users who were affected by vendor lockout, it's quite on the contrary. We find it very helpful and it streamlines the whole process. We don't need to go to court to forbade them to disclose this kind of information. What is your stance on this kind of transparency and especially from this perspective of end-user safety and how to construct the internal regulation policy documents for such procedures, so this can be balanced?

RAM MOHAN

Okay, who wants to take this question? Gautam is hovering over the mic.

GAUTAM AKIWATE

I can try. I don't have a specific opinion on the ADC transparency, but generally, having sort of done a bunch of research on a lot of

DNS security topics, I think what we have sort of come to the realization of like that more transparency is better. And what that usually means is this balancing act between how more transparency means that there is more data for attackers, but generally also means that like sunlight is the best disinfectant sort of thing where because CCDs is now available, a lot of our research was possible. We found operational risks that existed for a very long time.

And so, I think while I'm not answering your specific question, I think our general view has been and with the DNS transparency work party generally has been more transparency is good and how do we sort of enable more transparency while balancing privacy and security risks and making sure that threat actors are not taking advantage of the data. And we're also happy to chat more if that's helpful and sort of figure out like if there are specific questions and how do we chart the path forward.

MACIEK PIASECKI

Thank you very much.

RAFFAELE SOMMESE

And I just want to add there that in the work part, we are also discussing about access model to mitigate also risk for users. So, that's part of the discussion.

JONATHAN ZUCK

All right, Rod. Happy birthday.

ROD RASMUSSEN

Thank you. Not quite yet, but almost. A day after tomorrow, actually. So, I've actually raised my hand on another aspect of transparency, but as the lead member of the PDP from the SSAC, the topic that got brought up yesterday about the transparency of what things were done and part of an ADC was really interesting. And it is an interesting discussion point because as you mentioned, you don't want to give away the secret sauce of how you find a bad guy. At the same time, you're getting people swept up with false positives. You want to understand why and how to correct that problem.

There may be ways, kicking this around, of thinking about categorizing things. So, for example, if you did a registrant or account level ADC type, that might be listed as cross-checked registrant. And if you did some sort of technical thing like name servers or you knew of certain patterns, you might just say technical check or something like that, at least get you some level of categorization. That might be something to potentially explore.

When I want to raise my hand on this, just for bringing attention to this transparency work we're doing in the SSAC to the ALAC, is that there is an end-user impact, at least for the anti-abuse potential usage of a transparent DNS transaction base. This comes in particular when you have short-lived domain names that may not even appear in zone files today. So, depending on where we come

out with recommendations on that, there may be a recommendation or two that might be a fairly heavy lift to help support.

So that is something to be aware of, the ALAC, as we come up with that work, that we may be collaborating with you to help evangelize a certain position. We don't have a position yet. I want to emphasize that, but I could certainly see the potential for that, and that would definitely be in the interest of end-users for their protection. Thank you.

JONATHAN ZUCK

Thanks, Rod. I think that's it for the queue, Ram, if you want to continue on.

RAM MOHAN

Okay, thank you. Let's go to the final slide on this area. We also wanted to share what else we're looking at doing in this calendar year. Some of you may have watched us yesterday being part of the plenary on AI and its impact on DNS abuse. That seemed to be a pretty well-attended session, and we received good feedback on that. I just wanted to quickly share with you on that plenary, if you can go to slide 14, to give you a sense of what the community's responses were on the various questions that were asked in front of the community.

So, if you look at this one, 118. I mean, all of these had close to 100 responses from the audience, so pretty representative of our

community. I won't read everything on the screen. The graphics do a very good job of it, but this was the first question that was in the plenary that we asked, and you see where the concerns and the responses are.

Here's the second question that we asked, which aspect concerns you the most over the next one to two years? On that, the biggest one that was brought up from the community was 32% said more convincing phishing and impersonation attacks, which has a link to the safer cyber campaign that we're talking about, right? So, there's a plurality of opinion there, but more on that particular topic.

The next question that we asked was, hey, is it all good? Do we need to do much, or do we need to do a lot? It was kind of a split thing, some set of folks saying, yeah, we're pretty good, just have to do a little bit of an upgrade, and others saying, nah, we're not there. We got to do a whole heck of a lot, right?

The next question that we asked was, how should ICANN fulfill its stewardship role? And that is actually not three, but that's 33 and 63 on the numbers there. But that gives you a sense of the kind of overwhelming response was ICANN needs to understand the technology and monitor its use. This was carefully worded. It was not ICANN or, it was ICANN, the community, right?

And this last question is also aimed at the community. What role should the community play? And quite a number of folks thought the community should support development of technical

mitigation frameworks, and another said, who talked about expanding policy expectations around DNS abuse responses?

So I thought these were interesting inputs from the community or feedback from the community. So I just bring them to your attention as it was not only the folks who were in the room speaking and the panel that was speaking and responding to audience questions, but this is actually what many of the people in the audience also spoke to.

The other thing, going back to slide nine, the other thing that we're also looking at is continuing the conversation that we began at the plenary in ICANN85 on strategic resilience across the ICANN ecosystem. That's an area that we're pretty concerned about because we believe that we're now in an era where stability is not about keeping the lights on. Stability is not about just redundancy, right?

Stability and resilience is about how do you recover when there is a significant, sometimes catastrophic, but a significant event, right? And how do you make sure that the systems that you're dependent upon work? And who is looking at cross-sectoral dependencies? The power companies depend on the internet being up in order to coordinate power outages, but internet companies depend on the power system being up in order to coordinate internet outages, right? So you have that kind of a set of issues there.

As Rod was saying, we're participating in the DNS abuse PDP, the first PDP on associated domain checks. And Rod, I think you spoke to it. Did you want to add anything further to what you had said?

ROD RASMUSSEN

Just a general observation is that I think that this thing is progressing along at a good pace and that so far, at least from an SSAC perspective, we haven't seen any showstoppers. There's obviously things to iron out. And I'm of the belief that a lot of the real work is going to be in the implementation advice rather than the actual policy wording. Policy wording is important, obviously. And then that's where the SSAC is looking to really contribute a lot is in our expertise and knowing, for example, how to be effective at pivoting on things and what's useful and what's not, and maybe some work around metrics.

I don't remember who's on the ALAC team for that, but I know I've had conversations with a bunch of the other team members. So it'd be great to coordinate a little bit on what we're doing as well. So let's make sure that happens. We'll have sessions tomorrow, so we'll do that there. Thanks.

JONATHAN ZUCK

Yeah, I have quite a couple of questions. Oh, sorry.

CLAIRE CRAIG

Sorry, just wanted to identify the ALAC reps on the DNS. Can you please stand. Steinar, Kathleen, our members, I'm a participant,

and Eunice, please stand. Okay. So now you know who we are and we will reach out to you and you can reach out to us. I'm Claire Craig, for the record.

MACIEK PIASECKI

I'm Maciek. I'm an observer.

ROD RASMUSSEN

And we have also Jothan is an alternate. There we go, Jothan. And Matt Thomas is our other member, but I don't think he's in the room. And then Gautam is also an alternate. He's over there in the corner. So we all have at least some faces. Let's actually try and get together and have a chat and see where we all are and how we can help each other out. Thanks.

RAM MOHAN

Thanks. The other area that we're also involved in is the participation in the Review of Reviews group. Robert, did you want to speak to that? He's not here. And I don't know who else is here from the Review of Reviews work.

JONATHAN ZUCK

Have you been talking about it internally and feel good about where it's headed? I mean, there's no longer a Security and Stability Review per se, but it's moved either into the main bucket of accountability or into the on-demand. I don't know if that's

something you guys have discussed internally and how you feel about it.

RAM MOHAN

I'm sorry, Jonathan. I'm at sea on that question. We had a bit of a discussion earlier today about this. Tara, you were there in the room. Did this topic, what Jonathan brought up, did it come up?

TARA WHALEN

Jonathan, can you repeat that for me, please?

JONATHAN ZUCK

Perhaps you haven't had that conversation yet amongst yourselves. I was just going to say that one of the issues is the disposition of the Security and Stability Review that used to be a separate cadence review and is now out there as either an on-demand review or potentially put on the agenda for what's being called the Accountability and Transparency Review. And I didn't know if you'd had a chance internally to discuss that change about whether or not you thought that that was a review that ought to remain a static and cadenced review, or you felt comfortable about the fact that it's become more of an ad hoc review.

TARA WHALEN

There's been, I would call, maybe identifying the cadence as an issue, as something to be looking at, but I would probably say we haven't fully. I mean, the discussions that we had today were more

sort of high level and identifying particular issues and not sort of delving into sort of solutions around cadence, really, I say, is the best way to describe it.

RAM MOHAN

Thank you. And Suzanne, thanks for raising your hand on Zoom. Glad you're here.

SUZANNE WOOLF

Yeah, I'm sorry. I went back to my hotel to get some medication, so I'm temporarily. But yeah, I mean, I think Jonathan's asking a good question, and we did have a fairly lengthy discussion this morning just about the current status and some of the issues that were raised in the public session yesterday and so on. I think a fair amount of what we ended up talking about was that people are not necessarily entirely clear on how specific scenarios might work.

And there was a notion that I hope we can follow up of sort of sketching out some scenarios and going through the current proposal and seeing exactly what happens. For instance, if the mechanism to make sure that security and stability reviews can still happen if the mechanism is strong enough and people are willing to make sure that works, that's not necessarily a problem to not have it on a cadence.

And people were willing to be concerned that the reason we're doing the review of reviews is that the way reviews were being done had these weaknesses that I think everybody has encountered in

one form or another. So I think where we left it is the idea of sort of sketching out in a little more detail exactly how specific cases might work, and sort of proceeding from there on whether we think the proposed mechanisms are adequate. Thanks, Suzanne. Robert?

ROBERT GUERRA

Yeah, sorry, I just had to step out for a moment. Again, it's Robert Guerra for the record. A lot of stuff's been said. I'll just say that the draft is out and there is an expedited timeline compared to many other cross-community groups. And so I would very much suggest that the ALAC look at the draft and send in comments. Some of the reviews could include the ALAC itself. And so how you would like that as well, any way that if there's an interest to perhaps some of the folks on ALAC working on this, want to meet with Suzanne and I, please let us know and we can maybe share notes. And I think having common comments from different SO/ACs would be much helpful. Thank you.

RAM MOHAN

Thanks, Robert. Let's go to the next slide. This is the other topic that we had teed up, which is a brainstorm. Jonathan, I'm cognizant of the fact that we have successfully managed to use up the time again quite a bit. But thankfully, we've discussed some of this before.

I'll just flip to the next slide to just give you a sense of what we're doing with the ISPCP. It's a different kind of outreach that we're doing with ISPCP. And what we did with ISPCP is, and this was with intersessional meetings with them, we came up with an editorial calendar, if you will, for the entire year. And we listed topics and the topics list actually originated from the ISPCP to us. And we were able to then kind of curate those topics.

And at the ICANN85 meeting, we had two sessions. Here at the ICANN86 meeting, we have a couple of sessions as well. So, there is kind of a specific focus and topics. And in each of these topics, the way these sessions run, and we're evolving on that, but for each of these topics, the SSAC provides the experts, the SSAC provides the speakers, right? The ISPCP provides the audience, the coordination, the structure, the Zoom calls, all of that is done by them. And our people prepare, show up, speak, engage, and then we're on to the next. So, that just is an idea of what we're doing with ISPCP.

But I'll hand it back to you, Jonathan, for the brainstorm on Safer Cyber and perhaps what we might be able to do collaboratively.

JONATHAN ZUCK

Thanks, Ram. And I think we're going to, like I said, we've been sort of getting the rest out of our own communications pathways with the phishing course. And so, that course is evolving, is going to get translated in the different languages soon. And I think we took the position that I think was reflected by you that we should get out

what we have and not make the perfect the enemy of the good, but at the same time, look for opportunities for it to evolve in the context of AI and things like that.

So, we ought to figure out what, if anything, AI changes about what end users should know, except that things are just getting better as a result of AI. And because what we used to call spear phishing could become much more widespread as a result of AI, for example. But then I think we should probably go through a list of topics with you at some point and look at them from an end user perspective.

And again, not to forget Pari's point, look at them from a policy perspective as well. In other words, look at the things that you're reporting on that could easily become the PhD that ends up on the bookshelf and doesn't find its way into policy directly, because we have a role to play there as well, whether it's requesting an issue report or doubling up on advice to the board, etc., to take action on a particular topic. So, there's ways for us to amplify messages internal to ICANN as well. And I think going through the list on that would be fruitful.

The other thing I was going to ask you about is whether you, as a group, have had an opportunity to digest the latest inter-RALO report, because my understanding is that the likely pushback from the registrars is to be critical of the reputation block list as a source of information. And I'm wondering whether or not you share the concern that we may need to find another way to measure DNS

abuse than these RBLs, or if you think that's largely an empty concern.

RAM MOHAN

Thank you, Jonathan. I think in terms of next steps, I think we should take an action item between the ALAC and the SSAC on originating a set of topics. And I would say also that we should get a meeting on the calendar, intersessional meeting on the calendar between here and ICANN87, at least one meeting, so that we can do some planning for it and get an agenda put forward to that. And no, we've not discussed the inter-RALO report. It's very new, and it just hit our list earlier today. So there's been no discussion about it. Thanks. Amrita has her hand raised.

AMRITA CHOUDHURY

Thank you, Ram. Sorry, I'm coming in many times. I'm just looking at the schedule you have with ISPCP. We have our capacity building sessions, we have our policy forum sessions.

Perhaps we could, if we have joint discussions during the time, we can also have a smaller, lighter calendar wherein we can pick on issues mutually and have those kind of discussions or webinars where your experts also come and speak, some people from our end user perspective speak, so that we can have some conversations, people across the globe who are our members or who may be from any of the constituencies can come in here because capacity building outside as well as capacity building of us

is important. So perhaps this could also be something which you, Jonathan, may want to think of.

JONATHAN ZUCK

Yeah, I mean, I think actually we keep talking about the ALAC. I think probably the intersect point between the SSAC and the At-Large community is the ACES group that Amrita heads up. That I think is going to be the best conduit to go back and forth. And so having an intersectional meeting sooner rather than later between the ACES group and the SSAC I think would be a powerful meeting. There's representation from all of the regions on ACES and that would probably be a good next step for a meeting.

RAM MOHAN

We're happy to do that. But again, what I will say there is the action will be on your end and invite us and we'll show up. But it's unlikely for us to follow through with you. Thanks.

JONATHAN ZUCK

Gisella, who's on the call, is writing down this action item right now as we speak, I'm sure. Thanks. One of the final questions I had for you. We're almost out of time. One of the issues that is faced by contracted parties is vast differences in resources between, say, registrars. I mean, a lot of focus is on them in the DNS abuse space. Do you think there's a scenario under which ICANN could directly or indirectly be involved somehow in the creation of tools in the AI

space or something like that that would be then useful across the spectrum of registrars and not just benefit the ones that are bigger?

RAM MOHAN

I'll provide my own personal perspective on it. Inside the SSAC, we have, say, registrars, some who are from large organizations and some who are small. And I don't know, what I hear is that it's not just the resources, but it's a prioritization issue inside of both large and small organizations, right? There's a kind of an endless list of tasks that they have to work on. And picking the important ones when the urgent ones always are crying out for attention is really what I hear is a significant problem.

Personally, I would be a little skeptical of ICANN the org coming in and, quote, unquote, helping the registrars. And it's one of those where the government were here to help you type situation. But that's just my personal opinion. We have some members who are registrars here. Please speak up if you'd like to. Billy says no, and Jonathan is not saying anything. So, okay. And Rick, please.

RICK WILHELM

I'm part of a registry. It's highly unlikely that that would happen for a staggering number of reasons. If anybody's really curious, you can just find me in the hallway.

JONATHAN ZUCK

All right. I was just spit balling. I'm trying to figure out how to bridge the gap between the haves and the have-nots in the

contracted party community. But we'll have to think about that further. Maybe it's something that happens outside of ICANN, but within the community, with the grant program or something like that. But in any case, I think we've hit our time. But I think it's been a great conversation. And we will take on the action item of initiating an intersessional session in the not too distant future.

RAM MOHAN

Thank you, Jonathan. Appreciate it. And Danielle, we have helpful feedback on our slides that we need more cats. So, we'll have to see what we can do there. But with that, thank you, and appreciate your time. Hope you have a good rest of the meeting.

JONATHAN ZUCK

Thanks, everyone.

KATHY SCHNITT

Please stop the recording.

[END OF TRANSCRIPTION]