ICANN81 | AGM – Joint Session: ALAC and SSAC
Sunday, November 10, 2024 – 13:15 to 14:30 TRT

YESIM SAGLAM: Hello and welcome to the joint meeting of the ALAC and SSAC. My name is Yesim Saglam and I'm the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior, and ICANN community anti-harassment policy. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, French, and Spanish. 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. I will now hand the floor over to Jonathan Zuck, ALAC chair, and Ram Mohan, SSAC chair. Thank you.

JONATHAN ZUCK: Thanks, Yesim, and thanks everyone for coming. We always enjoy these meetings. There's a lot of alignment between the At-Large community and SSAC in terms of objectives and goals, because we're all out to improve the experience of users in large measure. So we have that shared commitment. And so we always enjoy learning what SSAC is working on, and as we are approaching the next round of new gTLDs, I think the intensity of conversations of what things need to happen to

precede that round is going to go up, and so we're curious about name collisions and things like that that affect that round, and as well as what we call these evergreen topics, such as DNS abuse, et cetera, and what you've been doing on that as well. There's a report coming very soon that was supposed to come before this meeting, the Enfirmal report that I was hoping we would get a chance to talk about, but we haven't seen it yet, so that may cut that conversation short, but it might be worth talking about it in some vague terms, I don't know. So welcome, and thanks for coming. Ram, go ahead.

RAM MOHAN: Thanks. This has become my second home here inside of ICANN, so really great to be with all of you. Like you said, there's shared values and also shared intent in terms of what we're trying to achieve, so that is what really animates us. In addition to the evergreen topics, we also wanted to provide you a briefing on some work that we have done and a report that we published earlier this year that is focused on DS automation, part of DNSSEC, DS automation, and we have an ask of you in that area. And then while we don't have a work party that has chartered specific work in this area, we do have some expertise contributed by some of our members that relate to AI and DNS abuse, and so we have some thoughts in this area that we hope will provoke a discussion here, because it has, I think, clear implications for users of the internet going forward. So those really are some of the big things that we're thinking of sharing with you about. It's also been, I wanted to report back to you that with Matthias as your liaison into the SSAC, it's just been delightful. There's been a great deal of engagement, and he's

helped prompt this two-way communication that we began a little while ago and that I think is starting to thrive right now. Thank you.

Okay, let's go to the next slide, and Jonathan, here, instead of putting together a large deck and do things like that, I thought really two things, and Merike is here at the microphones as well, but one of the things that prompted us to work alongside you to build Safer Cyber is our realization that we have technical expertise, and then we take the technical expertise, look at topics that are important, that we believe are important, and produce reports. But our big realization was you cannot think that the work is done. That's actually where the work begins, and the real rest of the work has to be about taking, not just disseminating the report as is, but distilling the key parts of the report, the key learnings from that, not just the recommendations to the board or the community, but the key learnings that are there, and finding a way to transcribe, to translate, and to make it accessible to the audiences that really matter.

So we currently have some work that we've already begun on phishing and those areas of online harms, and I'm really pleased with the progress that we have made in that area. So I thought, Jonathan, maybe we can spend a little bit of time speaking about that work that is already in progress, but then devote the rest of our time speaking about when you and I spoke, we had this vision of a Safer Cyber campaign that would have multiple parts to it, components to it, and we've done work in a bunch of other areas that I think may have relevance to the users of the internet. So I thought perhaps we might have a discussion about

what other things might be useful to think about as the next pieces of the Safer Cyber campaign that gets us into 2025. Thank you.

JONATHAN ZUCK: That makes sense, Ram. As far as an update, we've created most of a course on phishing in particular and Safe Cyber, and that you've had a chance to review. We did a demo of it here at a previous meeting, and you requested that smishing be added as one of the things that we talk about, even though it feels less DNSSEC, I guess, but I think that's not something to worry about outside the ICANN world. We should just worry about what the users need most from us. And so we're working together with the designers to add that. We also, Sébastien, who does some teaching of senior citizens, I think, in France, translated it into French, and did a little workshopping of it as well, and had some feedback in terms of like its clarity for less sophisticated users and things, and so we're making some updates there. And ICANN had some feedback in terms of basic accessibility, like contrast ratios and things like that, that we're working together with the designer to get that implemented. I think we're in a position to kind of launch this early in the new year. I've been in discussions with the Library Association and they're interested in teaching this class as well. And then we're working out our own processes for review by our regional organizations to see if there's regional changes that they wanna make, and then hopefully press that out to ALSes for them to be able to deliver it there. So we're hoping to achieve something similar to the success of UA Day ourselves with the delivery of this, but also looking at partners for delivery of information out to the typical end user.

RAM MOHAN: Wow, that's substantial. And I'd be very curious to also hear about the feedback on that you heard, Sébastien, on how to bring even greater clarity, because that's something that we really care about as we, one of the things that we're starting to do, Jonathan, is on our evergreen topics, we're looking to bring out maybe a 500- to 1,000- word executive summary. Think of it as a briefing paper, if you will, that actually collects the work that we've done together and collates it, puts it together in an accessible way that, again, perhaps can be used as source material or as a base to start conversations with those who are uninitiated in, for instance, DNSSEC. Or uninitiated, for instance, in blockchain and the DNS. right, things like that. I think we would love to learn quite a lot from how you're improving the communicability of the messages that you're trying to get out.

JONATHAN ZUCK: There's a lot to learn from the history of direct mail, direct marketing in the U.S., and that they never just sent something to their whole list they'd send it to a little bit of the list and get feedback and modify it and send it to a little bit of the list, and I think that we'll try some experiments like that to try and figure out what messages get across, and I mean I think experimentation is going to be the name of the game here, and we may need to create TikTok videos or something to convey some of this information in very bite-sized pieces, because generally speaking getting the people in this room to read a thousand words might be difficult. So a little animation or a clever way of getting people to, sucked in to learn more might be part of the exercise as well. I see

Sébastien's got his card up if you want to share some of the experience that you had. I didn't mean to put you on the spot when I brought you up.

SÉBASTIEN BACHOLLET: Thank you, Jonathan, to recognize my work. It was not too much my work, but work done by the people I deliver the course to them, and it was, for me, it was a test for us, because it was with senior people and where they have trouble to understand. Part of my job was to translate it in French, and when you translate to another language, you have also to take care of how it's written in English. Therefore, I really suggest that before you send anything, you ask your colleague or you ask us to do a translation in, if it's a short document, because it can be useful, but we don't need a professional translation. We need a translation who will be targeted to the people who we'll be speaking to. And one of the difficulty we have with interpretation and translation, it's the language you use in English, not you, we use in English, and you, when it's your first language. Sometimes you consider that the word, it's an okay word, but when we get it, it's not the same. Therefore, the word we use, the complexity of the wording, or the simplicity of the wording, therefore I used to say we need first to translate into simple English, and then to translate to other languages, because it's the first step we need to do. I tried to do both at the same time in going into French, and then I come back to English.

And what is important, what Jonathan just said, we need to cut this presentation in pieces, because it's really very difficult to explain what is the difference between this type of phishing, this type of, the

translation in French, it's quite complicated, and therefore, and the image you give with, in English, don't work in French. The image, the word you use, why phishing, why, I don't remember even the word, but the one under the sea, or whatever, you use different words, and it's impossible to translate into French. The image you have in English is very good. I have not yet totally found a good image in French, and I guess it will be the same for other languages. Therefore, it's communication, Jonathan better than me, it's quite complicated, but let's start with something about language that can help us for the rest, but once again, the work done by Jonathan to put the first, really was very, very interesting and very good, and it's a good base to start to work here, and thank you for allowing me to do that in French and to my peers. Thank you.

JONATHAN ZUCK: Thanks, Sébastien, a lot of it is experimentation, and we're going to find out what works. I mean, one of the things we put together, as we try over the next couple of years to experiment with, there's words that are kind of loaded, because they're sort of part of our bylaws and things, but if I can say little o outreach, right, outreach means something very specific to the At-Large, but the idea of kind of using this whole communications pathway we have, this infrastructure that we've put in place to get to as many people as possible, and what does that look like, and there's a lot of different ways that could happen, and I think that as we look at some of the things that you might, messages you might want to get delivered, some of it may come down to the audience, right, who is actually the person to hear about this? So as we look at something

like universal acceptance there's these courses that they've developed, which we're sort of modeling what we're doing after, but we also thought, well, does it make sense to do a Twitter campaign or a X campaign or whatever, a social media campaign in which we try to get as many people as possible to mention, say, a major airline that isn't yet UA compliant, right, and try to get as many people to deliver the same message that we know that somebody there understands, we find out who the person is and target them in a large institution, and in the case of DNSSEC, the typical end user isn't your final audience, which what you're hoping for is to leverage that constituency to deliver that message to their IT manager or something like that, right, and so figuring out the audience and how we're trying to get to them is going to be part of the exercise as well. Thank you, and on the SSAC side, now when we produce reports, we're also thinking about which of the audiences that report has resonance with and which of the audiences who we didn't even think might need or might want, and therefore we didn't write for them, we didn't even think about them, but we actually find that they're the ones who've taken it, adopted it, and have used it, right, and there's actually quite a lot of learning from that because in the earlier days, there were several reports that we wrote, and the biggest pickup of that report was in the ALAC, right, you took it and then you ran with it, and that kind of led us to think, oh, maybe we ought to integrate more with that point of view, right, so that's really valid. So you'll see us getting better at that for sure.

Now, currently, we are working on two topics inside of the SSAC, and it just so happens the co-chairs of each of those topics happens to be in the room. One is on DNS filtering, a refresh on that. We have earlier

spoken about DNS filtering, but we are refocusing on that area, and we're beginning work in that area, and we're also looking at open source and the implications of that on the DNS. So those are two current areas of work inside of the SSAC. If you have other areas that you think are important for your community that either we should initiate new work on or perhaps take work that we've already done and purpose it in such a way that it reaches your audience, speak to us about it, because we're open for that.

JONATHAN ZUCK: Definitely.

RAM MOHAN: Okay. Let us then, if anything more on this, because really what I want to do is I want to put this as a marker to say Safer Cyber isn't a 2024 project. Safer Cyber is a joint SSAC-ALAC campaign that we go and we build and we run over the course of our future beyond my term, beyond your term. Okay, great. Let's go to the next slide. So we have Peter here to share with you insights from a report that we published earlier this year, SAC-126, and I'll hand it to you, Peter.

PETER THOMASSEN: Yes, thank you. So probably some of you recall that we've talked about this before, but at the earlier times when we talked about this, this report was in progress. Now it's done, and I will give you a quick summary of what it says and why it says that. So when you want to use DNSSEC, you need to put a link to the child domain's DNSSEC validation

key into the parent zone so that you actually have an authentication path, a chain of trust. The way this works when the registrar is the same organization as the DNS operator of the child domain is that it's done internally and not very, like it's a one-party problem, so to speak. The registrar can just do that themselves. But when the registrant has chosen a different DNS operator, then it's a multi-party problem. And the way this works today mostly is in what we call the registrant-centric approach, where the registrant has to fetch the cryptographic key parameters from the DNS operator and then somehow bring them up to the registrar. And that might involve going through a reseller.

And it's all not too easy, in fact. There's different kinds of interfaces that sometimes seem contradictory, depending on the TLD or the registrar. And there's also various types of inputs, formats, and stuff like that. So it's in no way straightforward. And if this was automated, I guess it would be better. And so the SSAC did investigate this problem space in the SAC-126 report. Next slide.

Yeah, so as I said, this is essentially the problem statement. And yeah, we can go to the next slide. The report gives three recommendations. So it investigates the solution space that exists today for automating the DS record provisioning in the parent domain. And it finds that there is just one standardized method with an IETF standard. That's the CDS-based approach, where essentially the child DNS operator puts tentative DS records into the child zone. The parent can discover them and publish them. So that's RFCs 73 44 and 9615.

The first recommendation of the report says that if any registry or registrar wants to use this method, or wants to do DS automation, this

is currently the recommended method. And it does have some limitations. So for example, it is not the most efficient way conceptually for doing it, or it doesn't really say yet what happens if there is a registry lock, for example. Should you be continuing to do this automation or not? But anyway, this is the currently recommended method. Then the recommendation two says that it would be helpful if ICANN org supported registries and registrars who want to use this, and not make the process too complicated. So currently it requires kind of a feature request from registries to be able to deploy this in RSEP. And it would be nice if, for example, the fast track RSEP could be used, which is not as costly as the full RSEP process. And yeah, so we'd like to encourage ICANN Org to move this forward with those registries and registrars who do want to use it.

And third, I did mention operational considerations, like what happens when there is a lock, and there's other ones, like which kinds of technical acceptance checks and input validation should be done when such automated DS parameters are ingested by the parent, or for example, what should be the TTL that you set in a DS record in the parent, which governs the recovery time when you mess up and you have to undo it. It's cached for as long as the TTL is, so low TTLs might be a good thing to consider here. And all of that is not standardized. It might be inconsistent across TLDs. Some ccTLDs have deployed this automation already today, and they don't all treat these things the same. So we're encouraging ICANN Org and the community to find solutions that are consistent for such matters and can be applied across the TLD space in the same way. And then once that's done, I guess there is a more holistic, fuller solution to the problem. And so far, it's only an

incomplete one, but it's the one that's currently the one to use. That's essentially the overview of it. More details in the report, or if you have any questions, very happy to take them.

RAM MOHAN: So, yeah, I think there are two pieces to this, Jonathan. One is, we'd like to solicit your help. Look at number two there. Support registries and registrars by using mechanisms from recommended, facilitated FastTrack, RSEP. That's an area where we would love to get your assistance to help work with ICANN Org. Maybe we can help you understand why this is a useful thing, why this will improve the security and stability of the system overall. And then maybe, because in these things, more voices at the table help. Because as we know, with ICANN Org, they tend to be quite responsive to inputs from the community. And when they hear us speak sometimes, they can say, oh, that's the technical guys speaking. But when you combine that with a group that is not necessarily only technical, but has lots of other elements of interest, we think that may increase the probability that they will actually take that and do something with it. So maybe a joint letter or something like that.

JONATHAN ZUCK: In particular, you're thinking about a contextualized ask of Org to allow for fast track RSEP in this particular context or across the board? What do we think the ask would be? And is it something that would be directed at Org itself? Not the board.

RAM MOHAN: Right, not the board, it should be Org. fast track RSEP would be an example. We're not saying it should be that. The implementation of how to do it should be left to Org. But what we would like is to have something that goes to Org that has the heft of both of our committees behind it that says, this is an important topic. Please pay, not only please pay attention to it, but please begin execution of it. We believe, and we have already said fast track RSEP. So we don't need to say that again. But what we do need to say is. Prioritize it. Prioritize, this is important stuff.

JONATHAN ZUCK: Yeah. No, I certainly think we'd be open for that. Let's figure out a joint correspondence on that.

RAM MOHAN: So we have SAC staff here in attendance. John is here. So John, if you could please take that as an action for us and let's coordinate with the ALAC. And Matthias, maybe you could help as well. Keep us accountable on that. So that's a specific ask that we had in mind, Jonathan, this topic.

JONATHAN ZUCK: Well, that's an easy one. I mean, talking to a community that already kind of understands the underlying issues. Right, right.

RAM MOHAN: Well, we'll try and bring more easy things to you then.

YESIM SAGLAM: We have an online question from Eunice Alejandra Perez Coello. The question is, what end user documents exist to install DNSSEC on a recursive DNS? And if a SSAC consider important that the end user can install it on their LAN? Thank you.

PETER THOMASSEN: Okay, so this is Peter again. So the question included the observation that DNSSEC is deployed on resolvers for validation. So that's correct. And most current DNS resolver software does support DNSSEC validation and does have switches to turn it on. So some names of software that you could use are, for example, BIND resolver. There is Knot resolver, there is Unbound, there is PowerDNS recursor. If you want to use those, all of those have DNSSEC capabilities that are easy to switch on with just one line of configuration, I think. That aside, you could also use a public resolver, like the ones from Cloudflare or Google or Quad9. So those are 1.1.1.1 IP address, or 8.8.8.8 or 9.9.9.9. And also that aside, most people use their internet service providers' DNS resolvers. So most likely, your access provider, I don't know who that is, will assign a DNS resolver to your internet connection when you establish it, and then that will be used inside your LAN. So you can overwrite that by configuring what I just described. However, if you are interested in very low-friction DNSSEC capabilities, it would be easiest if your ISP did it for you. And whether your ISP supports it is hard to tell from this chair. So I don't know, you would have to ask your ISP and perhaps encourage them to enable it if they haven't done so yet.

As for documentation, which was your initial question, each of the things that I mentioned has documentation. So if you enter those names in Google Search, for example, of those DNS software products, or if you enter Quad9, for example, for this public resolver, you'll find how to set it up. But right here on the spot, I don't have an overview document that would summarize those options, although I'm sure there are some available. So if you email me at Peter, sorry, if you email me at Peter at desec.io, I can take a look and send you a recommendation later. Any other questions from the group here at the table or in the audience? Okay.

RAM MOHAN: Jonathan, this is the impact of having a session right after lunch.

JONATHAN ZUCK: Yeah, definitely is, definitely is. All technical sessions should be first thing in the morning.

RAM MOHAN: Okay, let's go to the next slide, please. I'm going to hand it off to Tara.

TARA WHALEN:

EDUARDO DIAZ: This is Eduardo for the record. We're just discussing here how this impact the end user because we as an end user, we are not registering,

or some of us are registrants and we are not registrars. In fact, this thing that was explained here, it went over my head, and I'm a technical guy because I don't deal with this every day. So it's very difficult for me at least to understand when you explain what DS automation is. So I don't know other people. But anyhow, that's why I wanted to bring it, that you're speaking to an end user audience. It's not no such technical, thank you.

PETER THOMASSEN: Yeah, so maybe the main takeaway from those earlier presentations and explanations that I should have made more clear is that the point of this automation is that it would be less complicated for the end user actually. And that it would be a feature that would be implemented by DNS operators of the child domain, like something.com, and the corresponding registrar to arrange for DNSSEC configuration automatically so that the end user does not have to concern themselves with it. And there is this particular problem of configuring the so-called DS record in the parent domain that currently involves manual interaction with the registrant. And the report suggests that that manual intervention, if it went away, would be easier for the end user. Thank you.

EDUARDO DIAZ: I follow up on that, but what do you mean in the end user here?

JONATHAN ZUCK: Registrant. This is probably an important distinction.

TARA WHALEN: Yeah, so if I may, I know some of this gets quite complicated, and many of the SSAC are very much entrenched in it. So if I want to enable DNSSEC, right now, what you have to do is you have to deal with keys, and they're private and they're public keys. And so right now, the registrant has to understand that, and they actually have to enter the correct information. And so that causes a lot of issues. So what we're trying to do here as SSAC is to automate all that, so as a registrant, as somebody that's going to say, I want my domain to be DNSSEC secured, all you have to say is, or click a button, and just everything happens. And so that is the main gist of it, so that the registrant, the end user, doesn't have to know anything. It's like getting your oil changed in a car. Just please do it. So I hope that maybe helps a little bit.

EDUARDO DIAZ: I understand that. Usually what you do is you talk to your host person, and they charge you for that. So they do it for you.

JONATHAN ZUCK: Yeah, no, it's an ongoing issue, because the end user and registrant distinction. And so in this case, I guess it's an end user of the, I don't know, of the DNS system or something like that, that needs to fill out different parts of information, switching servers. I mean, there's more and more of that that happens as people are using things like Squarespace and things and trying to redirect their websites to different website builders, and they're being forced to go in and edit their A records and things like that manually, which is this sort of

strange thing for a lot of, somebody who was just an end user until suddenly they wanted to have a website. So I mean, I think that distinction gets blurry there, but yeah, this is definitely about somebody with their own domain.

SATISH BABU: To me, this sounds like a very nice idea as far as registrants are concerned, because this takes out the drudgery in ensuring security of a particular resource. So if, as you say, you click a button and everything becomes secure, I think it's a very nice thing to socialize. I think ALAC should enthusiastically support this proposal so that the benefit of this goes down to as many people as possible. Thank you.

RAM MOHAN: All right, I don't see anything else online. So Tara, over to you.

TARA WHALEN: Thank you, Ram. I think Ram mentioned a bit earlier that the SSAC has been working on a number of technical topics for many years now, but there is this idea of evergreen topics. Even though the landscape changes a lot, there are certain topics we return to again and again. And we are trying to focus our attention on many of these and finding ways to sort of become a perpetual voice on these. We have our reports that come out, our advisories, but we also have other ways that we can communicate. We can have sort of blogs, we can have presentations to people, because people will come to us on these topics, and we'd sort of like to have it easy for people to access information on these topics

that you are facing on a recurrent basis. So these five topics are laid out here. You will probably not be surprised to see DNS abuse on there. Obviously, the DNS being a very important system is also a very important system for people that want to do online abuse. So this topic, sadly, we have not fixed the problem of DNS abuse, and so it continues to be very important to all of our communities. So we continue to have advisories on this, and particularly as these vectors evolve, then we are trying to evolve along with it and keep everyone up to date on mitigations, for example.

There's also the topic of new gTLDs, which is perhaps particularly timely right now. So you will all have the next round on your minds. Well, in the middle of all of these considerations are also security and stability considerations of bringing out new strings. There was a lot of work on name collisions recently, for example, so this is another recurring topic. And as Peter teed up very nicely, also DNSSEC. We have very core technologies around DNS security, and they are very complex as well, and often also evolving. And the complexity means they can be difficult for you to deploy correctly and without having some issues, and so it becomes important to provide information to the community about many of the complexities and finding ways, for example, like automation to perhaps make this job a little bit easier to make the security work in the way that it was intended.

Another topic is alternative namespaces. In the more recent discussions around things like blockchain namespaces, for example, you would have seen a lot of discussion around naming that does not involve necessarily the DNS. This is not the first discussion of alternative

namespaces, and those of you who have been around for a while are certainly aware that another universe of namespaces was possible outside the DNS, but we do have to find ways of figuring out how these work together, how they might integrate with the DNS, and what the particular security and stability issues would be between the namespaces, so this is an area that we continue to look into. And of course, there is Internet governance, particularly around security and stability of this issue, when you have a large piece of Internet infrastructure, there's a lot of technical policy issues that are happening around that, and when you have people making policy where there is an overlap between the technical and policy space, it can be important to try to provide solid, useful technical information to assist people in making those sort of decisions to the best of your ability, so we're sort of attempting to find ways where we can provide the sort of technical underpinnings, enough information to send out to those communities so people will have a better idea about what the, for example, the possibilities are and the limitations are of taking particular approaches around these technical policy decisions. A couple of work parties we have right now, I should also note that not everything stays in one box, sometimes there's overlap between the different areas, and we have areas beyond this as well, but two of our work parties that mostly are, for example, looking at some Internet governance and other security issues are a DNS blocking, filtering work party. For example, you are aware that there will have been efforts over time for these governmental or regulatory to mediate content access between users and a source online and using the DNS and interventions in the DNS as one of the methods of looking at this. Now, SSAC has written advisories

about this, but they're over a decade old at this point, and at this, during that time, both the regulatory backdrop and the technical backdrop have changed rather a bit. There have been developments such as DNS over HTTPS, for example, which means that the visibility of DNS queries to other parties is not as available as it once was, and so there have been changes made as to what approaches are taken for blocking and filtering. So we have decided to take a look again at that work and opened up a party, mostly again to provide information about what does the landscape look like, what are your tools, and what things are available, what side effects there might be that you weren't anticipating as you make certain choices about blocking and provide that out for people like policymakers.

We also have a work party on free and open source software in basically the DNS infrastructure. There are many components of DNS that could be things built into the recursive resolvers, for example, that are actually done by collectives of people or very small groups who are putting forth their time and expertise. They're not actually a large organized—they're not necessarily corporate groups. They may not be sort of well funded. They may not have contractual relationships with you, and yet they are really the ones maintaining and supporting large pieces of critical infrastructure in the DNS. So this provides a good, it's very good that these people are providing this information, that people may have assumptions about the stability of this, what things they can do when things go wrong. They may not have any idea about what their relationship is, what obligations may or may not be present, what things they are able to do. What happens when someone decides to stop maintaining something and it disappears? So the party is looking

at making some of these dependencies more visible, for example, and to make some clarity around the assumptions people have about the relationships that you may have and the dependencies on those pieces of infrastructure. I have a question from Jonathan.

JONATHAN ZUCK: Just quickly, not to interrupt, but are you going to just sort of raise this as something that we should be thinking about or make some recommendations? Should ICANN be more directly engaged with some of the—there's fun little cartoon memes about this problem. This whole tire stack and this whole thing the size of a toothpick being maintained by a guy in his kitchen that holds up the whole internet, and is that something we want to have change or create a net for or something like that? Do you think recommendations will be part of the work?

TARA WHALEN: So the work party is just starting, so I don't want to, again, speak ahead of if we have any of the chairs here who want to speak, but we can take a leap. So I mean, this is not a trivial problem in any way. I think when we can make recommendations, we like to do so. If there is sort of a clear mitigation, when there's a place where we can say here is a step you can take. And sometimes we are able, for example, to have a technical component where we say, this is a clear win, this is a thing that you should push forward, then we always will. When you have something that's more systemic, it can be more difficult for you to say, well, what would the solution be to working out, this, for example, is not unique to the sort of the naming system space. The issues around, I

guess, critical infrastructure and dependencies on open source software are broadly, I would say, they're a broader area than just ours. And I don't know that there has been a clear solution to how to deal with some of those. Sometimes there have been things where people will say, what can you do to help those groups? If you identify a particular group that are a linchpin for something, people say, all right, what might we do to provide them with resources? What might we do to give them more resources for making their own code more robust? There may be particular places where you can say, I would like this thing to continue, continue well and strongly, and direct yourself in that direction. But I don't want to jump ahead of where we're going to wind up in the party, because we're just getting ourselves started. But hopefully we will have some things, because it's always ideal, I know, when at the end of that you say, and we have a wonderful solution for you wrapped up in five simple recommendations.

SATISH BABU: Thanks very much, Satish, for the record. I have a question on number four here. I note that there is a parallel session going on about alternate roots. Now it says new namespaces should want to integrate with the existing one. Now whose priority is it to integrate? Is it our priority, or is it the alternate roots' priority to integrate with ICANN?

RAM MOHAN: Yeah. So we look at it not from that viewpoint. We look at it from the viewpoint of interoperability. If you have an alternate namespace, and there is utility in that namespace, and there is utility in another

namespace, a DNS namespace, for example, we think that maybe almost inevitably, but certainly there's a logical step that says people who are using those utilities in namespace one might want to integrate with utilities in namespace two. That's what we're seeing today with identifiers in the blockchain namespace wanting to integrate with the various identifiers in the DNS namespace, and there's work that's going on now in the IETF to try and get some guardrails and some formalism around that. So I think in general, once you have a namespace that has utility and value, users, it's the same set of users for the most part.

They then want to look for integration, and we think that there's more of that coming. And when those come, what issues exist. And there's an overlap. You know, you have in the blockchain space, for example, we have, it's in the public record, there are organizations in the blockchain space that have said they have reserved quote unquote TLDs. Now they're not TLDs in the way we use that that term here in the DNS space. So you have nomenclature collision to start with. But there's other security stability issues, right, with collision of what happens if names, identifiers that are existing and have a certain utility in that other namespace when another identifier that is the same exists in this namespace. How do you manage that. We don't have solutions for that, but we can see quite clearly that issues are going to arise. And we think part of our job is to raise the flag on that and say, must pay attention. If you don't pay attention, you will end up at a point where the first time you're looking at it is when the problem is already at hand.

OLIVIER CRÉPIN-LEBLOND: Just as a follow up on what you've just said, Ram, so I can understand ICANN being able to make sure that its own namespace is unique, and I can understand how ICANN can try its best to not have alternative or other namespaces clashing or being in conflict one way or another, but how do you then stop two third parties from clashing with each other? Because ultimately that might end up being also another issue. So there's no conflict with the ICANN namespace, but there could be conflicts between the alternative namespace. I find that to be a very far-fetched thing to try and attempt.

RAM MOHAN: And I don't think we should attempt that. You have various private parties that set up namespaces. I mean, you could set up all of the namespaces on your private network today. You could take every TLD that is out there and you could set it up locally. And your router will have a lot of fun when it tries to get out on the internet. But you could do that. There's nothing stopping you. So that's not our goal. Our goal is to say, should one namespace want to interact with another, what are the security stability issues that come up? And to give it the appropriate amount of priority and to make sure that you think about it and you design it right before you go about implementing integration.

SÉBASTIEN BACHOLLET: The question you raised, Ram, it's a very important one, but it's a deja vu. ICANN went through that a few times already on the alternative naming system. Therefore, it's not to say that things will not be going differently this time than before, but we have also to take into account

the history. So second is that I think, and I guess you raised this point it's how we call that. Because if we use our name to talk about the other, we will be stuck. And it's not because they use our word that we need to follow them. Therefore, if I may ask you something, it's to start to tell us how we can talk about them without using our word. Because it will be better for communication purposes and also to show that we are in two different worlds. And what you are talking about, it's how to protect our world to the impact that they can put in our, in coming to us and maybe disrupting things. Because if they want to do their thing in their own, that's life. Maybe one day they will take over to the system to communicate in the world, replacing internet. But it's not the case for the moment. Therefore, we have to protect, and it's not because we want to be a fortress, but because it's a system which is working well for everybody and particularly for end users. Thank you.

RAM MOHAN: Yeah, thank you. That's a really good point. Our approach is that technology is going to continue to evolve and we ought to embrace innovation. We ought to embrace these new technologies that come up. So we don't think that our role is to, as you said, Sébastien, not to make this a fortress and to protect it. We want to embrace it. But at the same time, there has to be clarity. If you're using terms, be clear about what those terms actually are. When you say, for me personally speaking, when I say TLD, I think of TLD as something in the domain namespace, but I'm seeing the word TLD also being used in other namespaces. That confuses me. When I hear resolver, it means something to me in this space, which is, in my mind, kind of the default common user space. So

it's that, there ought to be clarity on what those terms mean, and it's natural for folks in young areas of technology to adopt the nomenclature, the syntax, the language from established areas. That's a normal thing. What we really have to think about is if you have that happen and you go, you take it all the way to the end, if there is a failure in this other space and the failure in that other space is using all the nomenclature and technologies that are in this space, then when somebody talks about 2,000 TLDs failed in this space, what does that really mean? Resolution failed in this space, what does that really mean? So that's kind of where I think we do have to be, not protective, but really clear that these words that we're using are almost terms of art. They have specific meaning, and there is trust associated with it inside of this space. And there's nothing wrong with other places wanting to leverage and use the same feeling of trust, but we want to make sure that we preserve that trust and the integrity in this space.

OLIVIER CRÉPIN-LEBLOND: So are you effectively meaning that a name can only be a domain name when in an ICANN-accredited TLD?

RAM MOHAN: No, there are ccTLDs that have names, and they're not ICANN-accredited. But I'm saying if a name is in the root of the internet, that's a TLD, and when that name then delegates further names in it, that's a domain name. But what I'm saying is that if it's a name in a blockchain, you could decide to call it a domain name. And there's nothing stopping that, because these are not like intellectual property, trademarks, or

whatever. What I'm really saying is that if you think forward, and you allow this commingling of all the terms, failure in one space will inevitably result in collateral issues in the other space. And that's a stability issue. Please.

JUSTINE CHEW: Thanks, this is Justine. So that's a very good discussion that we're having. Two questions that I have in my mind is, can you clarify that this initiative that you're doing with alternate namespace, is that in collaboration with OCTO already? I forget, but so if you can clarify that. If it is, then presumably OCTO knows what you are thinking. Then the second question would be, how can the At-Large emphasize all these issues that have been brought up through this collaboration or this study to make ICANN do something about it? Thank you.

RAM MOHAN: Great questions, thank you. Yes, on this and other topics, we are in strong collaboration with OCTO. At the SSAC workshop in Washington, D.C., we had somebody from, we ran a panel on DNS and blockchain. OCTO was in that panel, contributing, participating. We share our research work with each other as it's being developed. So there's quite a bit of work there. What we have yet to do is, and which is becoming apparent in this meeting, because this is, I think, the third time I've been asked the same question, so clearly we have more work to do, is we've not done a great job of communicating that this collaboration and that the view of OCTO is somehow conflicting with the view of SSAC. It is different from the view of SSAC because OCTO comes from its

institutional home while we come from the home of technical expertise. So you will see a difference in that area. But in general, with the alternate namespaces of the blockchain, my interactions, our interactions with OCTO have been similar. OCTO also hasn't come into this saying, "Blockchain bad, DNS good." They've come into this saying technology is evolving and we ought to find responsible ways of integration.

Okay. We have about 14 minutes left in this session, Jonathan. So the AI and DNS abuse piece, why don't we plan for our next session for that? Because that's going to take more than 15 minutes to go through and then work on. Does that work for you?

JONATHAN ZUCK: It does. And these are sort of our greenfield conversations as well. I will say that the Enfirmal report has come out now. So I don't know if there's people in the audience that are reading it as we speak. And predictably it did conclude that introducing some friction into bulk registrations could have a substantial impact on malicious registrations. So that's something that I think we'd be interested in trying to coordinate with you to raise the prioritization of dealing with in the near term, like goosing the GNSO to reopen the DNS abuse small team and talking about this issue of bulk registrations in particular, I think, as an obvious thing to point to as a way to minimize malicious registrations.

GEORGIA OSBORN: I will try and be very, very quick. Georgia Osborn, I'm speaking in my own capacity, but as a new SAC member. So I wrote an academic paper

about blockchain domain names a year or so ago, but obviously now it's slightly out of date. Things have moved along since the last year. But I think what would be of interest to ALAC is we probably have three different users of these things. So the first one would be blockchainers. And then the second one would be people from the DNS community who are curious. And the third one would be the kind of speculative making money type user. And I think what's interesting for us is where the Venn diagram of blockchain based identifiers or blockchain domain names meets the DNS and exploring that crossover. So like potential problems, potential challenges. You've got the IP challenges, abuse challenges, name collision challenges, and also opportunities. So like with .art, for example, you can have it's a place for artists to preserve their work and authenticate it. So there's different things that happen there. So that's really just what I wanted to raise. And apologies for taking some time there.

JONATHAN ZUCK: A question in chat here. How can SSAC's work on DNS abuse prevention be made more accessible and actionable for everyday Internet users, especially in regions with emerging Internet adoption? I think that's a continuous open question.

RAM MOHAN: And really my response to that is help us. We need the help. We're not communications experts. We're actually recruiting and asking ICANN Org, we're working with Sally Newell Cohen and ICANN comms team to help us become better at this communication thing. There's clarity

inside of SSAC that producing technical reports is the beginning of our work, not the end of our work. But do help us in finding ways to make our work more accessible and also actionable.

JONATHAN ZUCK: We're down for that, for sure. I think we're all trying to find better ways to communicate. In a mere eight years, we were able to get ICANN to work and brief on different topics, little primers and things like that. So I think the pace is really coming along. And that may be another mechanism, is coming up with sort of one pagers on things like that that help to summarize, animations. We've learned so much. Even ICANN Learn, I think, is starting to make progress in that regard. I mean, five years ago, all the ICANN Learn courses looked like textbooks from the '70s. And I think more and more they're taking advantage of some of the advances in pedagogy that have occurred since then. So I think this is going to be a multi-front effort to try and get some of this information out to everyday people.

OLIVIER CRÉPIN-LEBLOND: since we have a little more time, I thought I'd ask a few more questions. And one of them was regarding DNSSEC. Well, the question wasn't what came first, DNSSEC or IPv6, but it seems that both are taking an awfully long time to spread worldwide. That being said, and I've heard these concerns mentioned many, many times, and I think they've been answered in a number of ways, but some countries are concerned about the DNSSEC chain of keys that relate to how the whole key management works, with the top of the pyramid being that unique key

held by, I don't even know who, well, is it the key holders in ICANN. There's some concern about sovereignty that goes around that, and that whoever holds that key could turn you on or off, or have some form of control over your domain. Is there anything that's being done to ease those concerns, or is any work being done on that through, I don't know, shared keys or whatever else that could be?

RAM MOHAN: Thanks, Olivier. Inside the SSAC, we have not studied that topic specifically, but I've certainly, it's in the public imagination, it's quite a good way to—I've seen it in the press, people saying the key holders have the power. They can turn off the internet or turn on the internet. And there are actually clear mechanisms built in to not have such things happen. But again, I think there's a significant communications component that is needed for that.

STEVE CROCKER: I'm Steve Crocker for the record. So I've been involved with the sequence of activity for quite a long time, as have several other people, including the very competent ICANN staff that oversees all of this. The fear that's expressed in some quarters that ICANN could control some countries' access to the internet by turning off the keys is a thing that we've encountered. I've encountered it directly in some conversations. It's such a straightforward and easy kind of thing to think about that it's equally well understood how bad it would be if that happened. And so it's deeply, deeply ingrained in the structure of ICANN and the operation that that would not to be abused. And there are a few specific cases that

have already been encountered. Well known, of course, is that the U.S. has had a very dim view about Cuba, for example. Both phone service and DNS service for Cuba have not been bothered with, not been tampered with over a long, long period of time. I've been in direct conversations with senior officials in Russia who've expressed, well, what would happen if ICANN took us out of the root? And you know, I'm sitting there thinking it ain't going to happen. And if it did happen, it would backfire in the most egregious way. And with some tongue in cheek, it has occurred to me, I haven't said it directly, that if they could force the U.S. to do such a dumb thing, that that would be a big bonus for them and that they should try very hard to sucker ICANN into doing something bad like that. And then Russia engaged in hostilities with Ukraine. And Ukraine sent, there's correspondence on this that's available on the web, Ukraine said, take Russia off the net. And the answer was a very polite, well, we don't really do that sort of thing. I don't think that there's anything that needs to be done, frankly. That said, a country that is thinking about these things also has control of its own keys, one level down from the root, and each level of keys can be used as a trust anchor. So those users in a particular country could configure their software or be encouraged to configure their software or directed to use those trust anchors as opposed to the ICANN root and all would be well. Thank you.

STEVE CROCKER:

RAM MOHAN: Thank you very much. Thanks, Steve. Yeah, there are many safeguards that are built in. Other questions?

STEVE CROCKER: Olivier, I expect you knew all of that, but this is sort of almost a set piece for education of the community.

RAM MOHAN: Jonathan, the report that just got published, we will certainly have that circulated inside of the SSAC. And perhaps via Matthias, we could initiate that conversation about joining forces and getting together.

JONATHAN ZUCK: Yeah, that would be great. I think the new round, while not technically relevant to DNS abuse in particular, I think when we have these rounds, it creates an inflection point that facilitates conversations taking place that might otherwise be pushed to the back of the line. And so I think we should encourage this conversation to happen in the near term, rather than treating it as something to put off until after the round or something like that. And so I don't know if you feel the same way, but that's sort of been our experience historically.

MATTHIAS HUDOBNIK: I just wanted to say, so I'm happy to, again, summarize then the output as I did and then distribute it also in the mailing list. And then there were questions, I think, and we can then start to engage. I think that's a good thing, thanks.

RAM MOHAN: That brings us to the end of this session, Jonathan. Thank you again for hosting us and for really great questions from all of you, terrific suggestions. We have taken notes and let's continue this conversation and this collaboration going forward. I leave this conversation with a renewed sense of purpose and vigor, so appreciate it.

JONATHAN ZUCK: Same here, Ram, and I definitely applaud the efforts you're making to increase the accessibility of the work that you're doing. I mean, it only makes sense to do that. Otherwise, it's like somebody writing a PhD and it sits on a shelf in a university library or something like that. And how does it become something that's consumable by a wider audience? And I think we share a desire for a lot of this information to be more widely available and leveraged to bring about change. So let's continue to work together on that. Thanks.

[END OF TRANSCRIPTION]