ICANN85 Mumbai | CF – Joint Session: CPH and SSAC
Thursday, March 12, 2026 – 13:15 to 14:30 IST

NIKKI SCHULER

Hello and welcome to the SSAC and CPH joint session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, The ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct Concerning Statements of Interest.

If you would like to speak during this session, please raise your hand and zoom. When called upon, virtual participants will be given permission to unmute and zoom. On-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace. I will now hand the floor over to Owen Smigelski and or Beth Bacon.

OWEN SMIGELSKI

I'm not in the zoom yet, so apologies.

BETH BACON

Hi, this is Beth Bacon. I'm the chair of the Registry Stakeholder Group. This is the meeting of the CPH and SSAC. Thank you all for coming. It's like good turnout for the end of the road. Thanks friends. So, we will go ahead and get started. If you're not in the

zoom room, please go ahead. Does SSAC or Owen, are you in the room? Does anybody have anything they want to flag off the top?

OWEN SMIGELSKI

Hi everyone, it's great that we're able to continue these meetings. I know there's been a little bit of a break, so I'm glad to see that the CPH and the SSAC continue to meet, because I think it's good for us to collaborate and have these dialogues.

So, here's the agenda up on the screen, and I think with that we will dive right into the next slide, or we're just leaving up there. Okay, DNS Abuse mitigation PDP-1, associated domain checks. So, it's kind of an open discussion, CPH participation, as well as SSAC participation. Do we have a designated person to speak about this from our side?

Yeah, we usually designate Eric from our side, but he's not here, and I don't think Natalie's online. I'm looking around, I don't think we actually have any of our -- oh, Luke, aren't you? You're an observer. Oh, Dennis is online. Okay, Eric will be here shortly, so maybe we start with Dennis.

DENNIS TAN

Yeah, thank you, Owen. Dennis Tang here, Verisign. I think the short and sweet on balance, I think we are off to a great start. We look at the question number one of the charters, what triggers the requirement of doing ADC, and I think there is, no, I think not. I

know there is a strong proposal for Working Group deliberations, so we'll see in the next weeks how that goes along.

Also, I want to note that there's a lot of conversation about the timeline, and again, I just want to, I think, repeat of what it's already been said. The timeline was proposed by staff to the Working Group, but the Working Group has ultimately looked at how we believe that work is going to develop our time, and then we are really eager to beat that timeline, so we'll put the effort into having a more shorter delivery date if that is doable. I think that's it for me, but happy if there's any questions, happy to answer.

OWEN SMIGELSKI Thanks, Dennis. I saw a hand over there from Jim.

JAMES GALVIN Yeah, I did. So, James Galvin, for the record, I didn't want to comment or say anything to Dennis, but I, sorry, I walked in a few minutes late. Have we said who the SSAC reps are to this thing? Okay. So, just so that you know, in making all of that clear SSAC does have two representatives that we have identified to go to this PDP, neither of whom are here this week, and since I actually, I would have intended to -- Jocelyn's not the rep. It's Rod and Matt.

Oh, Rod's online now. Okay, well, then he should speak here in all this. Just wanted to make that clear. Rod Rasmussen is one of the reps, and Matt Thomas is the alternate, so they should be part of all

of that, and if Rod's here, we should let him have an opportunity to speak. Thanks.

ROD RASMUSSEN

Sure. Thanks, Jim. I actually just got in on the call, so I didn't catch what was said earlier, but I was not in Mumbai. I had a different conference I was supposed to be at that, unfortunately, got canceled, so I was able to get into one of the sessions. We had our alternates. I know Jothan was there. I think he was there. He was intending to be there as well, but we have a, just to give you an idea of where we're at with SSAC, we've got two folks participating.

We have stood up a Work Party within the SSAC to help support our representatives within the PDP, so we're planning on having regular cadence to go along with the PDP, so we can provide as much input as we can with as much flavor as we can from the SSAC as a whole.

Obviously, we don't speak for the SSAC in any particular thing. If we haven't written about it, that's our mantra in general, but I think we can do a good job of helping out here, because we have said plenty of stuff in this area, so we do plan on participating and offering as much insights and thoughts as we can to the PDP. I do believe, as we already stated, that it got off to a pretty good start, I think, is my impression from what I've been seeing on the mailing list and what I have been able to follow. If anybody else on the SSAC who was on, thanks.

OWEN SMIGELSKI Thanks, Rod. So, so far, we don't have anybody here from the registrar side, so as chair, I'll step in. So, we have a little bit more participants. We wanted to make sure that we spread it out across various registrar models, so we have Volker Greimann, who represents a wholesale registrar. We have Natalie Howatson, who represents a corporate registrar internet, now Natalie Howatson is with Cum Laude. Eric is with Squarespace, and Carlos is with GoDaddy.

We have one participant, that's Reg Levy, a wholesale registrar from Tucows, and then our alternate is Theo Geurts, who's also a wholesale registrar. So, since there, we've been meeting internally. We actually, for the first time, we had a preference of all speakers for the PDP. We had to cut to a grading, scoring way to decide who could and could not participate, which usually we're trying to bang the stuff to.

BETH BACON The audio is cutting out.

OWEN SMIGELSKI Oh, is it? I'm sorry.

BETH BACON They're fixing it.

OWEN SMIGELSKI

Okay, they are fixing the audio issue, so I apologize for that. So, we actually, usually we have to really try and work to get people to volunteer. This time, we had way too many, which is good, but what we have also done is we have an internal team as well, too, that we're meeting.

So, while there are people who are going forth, it's certainly a collaborative effort that we have there, and then the one thing that we did have as an update, we worked together and came up with a straw proposal, which I don't have handy here. I don't know if somebody has anything to drop in the chat. There we go. Oh, that's not it. Oh, I'd send a message to Luke to see if he could grab the straw proposal, but yeah, one of the things we are concerned with is certainly, as Luke put in the chat, is we want to really make sure that it stays very narrowly focused, so we avoid scope creep.

I think part of it is that will allow us get the work done faster, but then also this isn't a boil the ocean type of effort where everybody's pet peeve gets thrown into that. So, I think with that, Jim?

JAMES GALVIN

Just one last point of clarity for me, James Galvin, for the record, representing SSAC here, but since I came in before and was a little hyped up and spoke a little bit out of turn, just for clarity for the record in here. So we have two reps from SSAC to the PDP. I put

this in the chat, but speaking it into the record. So, Rod and Matt, and Rod has spoken they're not here physically.

And Jothan is the participant in the parlance of the PDP, and Gautam is our fourth rep who is an alternate in all of that. So, just so that's clear and I recognize all of that. I will also just add to this discussion, since I can, the ICANN Board is now actively seeking to put up its liaison into this PDP. So, hopefully that process will come to closure here in a week or so, and so the PDP will also have that rep present.

I know that that formal request came in a while ago, and it seems the request got a little lost on the Board side, but it's been tweaked up. So, that'll all happen, too. Thanks.

OWEN SMIGELSKI

All right. Thanks, Jim. I just want to, for people in the room, as well as people online, Luke put the straw proposal into the chat, and this is just a very first rough version that we just want to put forth, demonstrating that we think this could be a very simple solution and not be a 15-page policy output.

The amendments, the DNS Abuse amendment to the RAA was literally one sentence. So, this doesn't have to be something overly complicated, and so this idea in here, and we've already had some feedback. Please, by all means, take a look at it. Give us feedback. Work on it because I know some people have expressed concern with how the word customer is used in there.

There're certainly things to wordsmith and work out, but again, we think that this is something that could be done very quickly, or not quickly, but easily in that. So, pause here and see if anyone has anything else. Oh, Jeff, go ahead.

JEFF BEDSER I think that, Jeff Bedser, for the record. I think that the point of a very clear, simple, around the associated domain check is a really good idea. I think there are concerns that too much specificity on how it's to be done will be very useful to the criminals we're trying to work against. So, in broad concepts, describing what needs to happen, I think is an outcome we're all very comfortable with, and very specifics would be something we'd be unhappy with.

OWEN SMIGELSKI Thanks, Jeff, and also I just want to say, before we go to Sarah, that we really do appreciate SSAC participation in this, and we certainly want to collaborate because while some of us may have some DNS Abuse experience working from a registrar's side, you guys have some other skills and expertise that we may not have, and so certainly we value that feedback in there, and so hopefully we can collaborate within the calls as well as outside the calls as well, too, to make sure that we are coordinated and aligned and leverage your knowledge and expertise. Sarah?

SARAH WYLD

Thank you. This is Sarah Wyld, registrar, vice chair for policy. I'm not part of the ADC PDP, but I'm following it along, and I guess I could have put my hand down already because you kind of said what I've been thinking about. So, there's two pieces to it, and one piece is for this PDP specifically, as we've just said. How do we come to something that's useful without giving too much information away?

And then separately, just a bit more broadly, something I've been thinking for a couple PDPs is we really appreciate the input from the SSAC, specifically as the PDP is in the early stages, building in that security perspective from the beginning.

I come from a privacy perspective. That's my job. My day job is privacy, and so we always think of data privacy by design and by default, right? So, in this context, also thinking about how can we build in security to our PDP work by design and by default, and I think that's something that we really turn to the SSAC for. Thank you.

OWEN SMIGELSKI

Thanks, Sarah. This is Owen Smigelski, and I'd like to highlight the bad actors are listening thing. The Registrar Stakeholder Group, as you may know, we have something called acidtool.com, Abuse Contact Identifier Tool. I think it's what the acronym stands for. That's a free service that the Registrar Stakeholder Group paid to

develop and host where you can look up registrant information, but it also includes hosting and email information.

We've announced it when we first initially announced it, and then when we announced a big upgrade initially at the Cancun meeting and then at the Dublin meeting. The next week, we got hammered by DDoS attacks, which the first time, okay, that's an outlier, but the second time, that shows that the bad actors really are paying attention and trying to do stuff.

Fortunately, we had to get to a new server after the first attack. We weathered the second one, but we had 200,000 concurrent requests kind of thing. It was intense. That's one of the things, make sure we don't give out the secrets about how to avoid this, because you don't want to provide a roadmap for the bad guys to get around that.

Anyone else? Now Gabe's over there saying it's going to be the third time. No, we haven't announced an upgrade yet. It's only when we do new upgrades that they come after us, but now that I'm saying it, of course, they'll probably go after it now. Okay, seeing none, I think we can move on to the next topic.

RAM MOHAN Well, folks, first of all, my apologies for coming late. I was unexpectedly pulled into another meeting that I was unable to get out of, so sorry to be late. I don't like being late, but there's a great team here that pulls things forward.

So, some of you may have attended the plenary that we had on Monday morning on resilience, but I wanted to make sure that we shared from the perspective of the SSAC some of our thoughts and initial takeaways from the plenary.

What was the reason for us to even go forward and have the plenary? This is because we, in our conversations inside the SSAC, we really think that internet resilience is no longer just a question of whether the packets reach their destination. It's a question of whether the system of trust that moves these packets can actually survive the plenary. Storms that are hitting it, right?

So, it's not just about technology. It's also about the hidden dependencies, dependencies on power, cloud vendors, global regulations that we all rely upon, but that we do not control. So, as we are moving towards a world that is driven by both AI and an expectation of total connectivity, understanding the vulnerabilities that are there in these dependencies is the difference between a minor inconvenience or a global shutdown, right?

So, that was the reason why we wanted to have this plenary, because we believe we're at an inflection point. You know, 26 years ago, 25 years ago, in fact, the reason why the SSAC itself came into being was because of 9-11, right? That was the impetus that had a few of us sit together and say they came after physical things this time. What would happen if they came after the virtual part of it, right? That was 25 years ago, and that led to the creation of the SSAC.

Now, we're 25 years later, and it's a different world. The internet is now critical infrastructure. It is kind of the utility layer, right? So, that was the reason, and our intent here is to raise the awareness of the topic first, and I want to bring it up here with the CPH, because all of you serve and do something really crucial that users just depend upon and assume you just do it, and one of the things that came about in the plenary was the realization that those who have responsibility to deliver critical infrastructure in their own worlds are doing as best a job that they can do, right?

But inside of the ICANN community, is there cross-communication happening? You know, should there be a tabletop exercise that brings registries and registrars and ISPs and other folks together to say when there is a significant disruption, it's not will your registrar be able to handle it, will your domain name continue to resolve, but it's actually what happens to that interconnected system, right? So, that's the focus of what the SSAC is trying to raise awareness and bring it into the community.

Now, I'll go quite swiftly to some takeaways from the plenary. So, we asked the audience, what will the largest cause of the next global disruption be, right? This is what we asked the plenary, and there's a plurality of responses, but you look at underfunded preventative measures and circular sectoral dependencies, massively increasing system complexity as well as software supply chain risk.

Next slide. We also asked if your region's primary power grid or cloud vendor went completely dark for three days, how confident are you that your services could survive it, right? And look at the answers there, right? You have 36% saying, I think we're going to be, we may be okay. And we had 34% saying we're going to be SOL, there's going to be a real problem, right? And so that was, again, telling.

And the last question that we asked was, looking at that internet resilience, what is our community's most critical blind spot right now, right? And 38%, the text is small, hard to read, but 38% said cross-sectoral dependencies is where there is a significant gap, right? So, what we're really asking here, and the reason why we bring this topic is twofold.

One, do you see the gap that we're describing? And do you see our community having a role in helping bridge some of that gap? We have to, of course, make sure that we scope it appropriately, we don't try to boil the ocean, we don't try to reproduce what everybody else has done. But is there a role for inside of our community to develop a resilience playbook or a survivability framework for the ecosystem? So, Jeff.

JEFF BEDSER Hi. Jeff Bedser. So, I tend to be the one who loves to point out examples, so you can really kind of set this into your own state of being. So, most of you follow the news, well, at least the industry news, you try to avoid the U.S. news if you're in the U.S. right now.

But there's been a series of cloud-based cascading failures that have had multiple impact across airlines and all types of things. I personally was visiting with Tucows in Toronto and then taking a bus home because my airline's systems went down for three days. It was a 13-hour bus ride, that's a personal impact.

But when you start looking at the cloud infrastructure and an over-concentration of cloud infrastructure, where there's cascading problems and systems start to fail, and other systems start to fail hours later, but you can't get the other system back along, the other systems reboot, and you start thinking about a lot of the newer players in the space that are coming up the next round are building their back ends in cloud infrastructure.

There's a confluence here, and it's not a confluence we're talking about as a hypothetical down the road. We're talking about it's happening now, and if we continue to have, you'd think after the first three or four of these cascading failure issues with the cloud infrastructure, they figured it out. Well, it's not. They're happening more often now, and they're getting bigger.

So, it's going to impact the DNS industry, but also you start thinking about where all these confluences of different types of problems come. Yes, does ICANN have any control over the power grid? No, we don't. But should we know about if the power grid goes down in California and IANA is unable to update the route for several days? Is that impactful? We should know that. We should know how that applies and how it impacts us.

So, this is really what this effort to start is. It's not about ICANN taking the lead in fixing the problems we have no control over, but at least being a coordinator for discussions about what can be done to understand.

RAM MOHAN Thank you. Any other SSAC members want to speak to this before we pass the baton back? Yeah, John.

JOHN LEVINE I entirely agree with what Jeff said, but I am always worried about mission creep, which is a chronic problem at ICANN. You know, basically, every page we write about this issue, we need to be crystal clear, like, what about this is unique to the DNS? Or is this just like a general problem? I mean, like pick any large company with a website and they have all the same power and details issues we do, which is fine.

You can say like, there's lots of other people who can tell us about this but does this affect the DNS? Does this affect the registry process? If you can identify stuff that's there, then we might have some contributions to make. But like I said, I'm worried about the usual ocean boiling issue.

RAM MOHAN Thanks, John. Suzanne?

SUZANNE WOOLF

Thanks, Ram. I was actually somewhat gratified to hear that everyone is worried about mission creep with respect to this topic because it's enormous. It affects everybody in multiple ways. But I said in the meeting with the Board the other day that the way to keep control over the potential mission creep is to look at what only ICANN can do.

And I think that ICANN's unique responsibility for IANA and the root zone and all of the supply components of that and the operational components of that would be a good place to start because nobody else can take care of it. It is uniquely ICANN's job to take care of IANA.

RAM MOHAN

Thank you. Jim?

JAMES GALVIN

Thank you. James Galvin for the record. Speaking as SSAC's liaison to the ICANN Board, I want to speak a little bit to this issue of mission creep and just point out one of the things the Board did this weekend was have its own discussion as part of the annual strategic review plan and process that's going on about what are we concerned about going towards the future? Are there anything that we need to change in our strategic plan or add to it for consideration?

We do have in our current Strategic Plan the requirement to maintain the security, stability, and resiliency of the internet

identifier systems. So, now the question becomes what that means. And we went down a path of thinking about disruptive technologies and what they may or may not have as an impact on us, which brought us down to the resiliency discussion, which, of course, as Ram was just describing, we had this quite in-depth and excellent panel session on Monday morning.

I think there's a step-in front of mission creep. Before we decide that we're in the mission creep, I think it's important to recognize that we have to care about what's happening around us and what's coming towards us. There are some very big disruptive technologies happening right now.

We've had one along the way blockchain technologies, if you will, which is still out there and still doing its thing. But AI is sort of the new thing right now, and it's the hot topic. And the question is what does it mean to us? And there have been multiple examples along the way. I can tell you over the last few days of bilaterals with different constituencies. AI was mentioned, I think, in almost every one of them as something to be concerned about.

And I think a fair question for us as a community is first to examine what kinds of things are happening that could impact us, and then the critical question is to figure out where is the intersection and what we need to address, what we need to look at.

I think Suzanne's suggestion is an excellent one because she's right. I mean, that is sort of the unique thing within our remit, but that sort of stands out because it's what we know today. But I think

a discussion, keeping open-minded about what it means to address resiliency is important here, and we should be careful to scope the mission creep bit after we understand the problem space. That's what I don't want to lose. Thank you.

RAM MOHAN

Thank you, Jim. So, with that, I'll pass it back to you, Owen, and Beth, because the question that we have for CPH is do you see the gap that we're describing? Do you see ICANN having a role in filling it? And we want to begin a dialogue with you. I see Michele has a hand raised or had a hand raised.

MICHELE NEYLON

Yeah, thanks, Ram. Michele from Black Knight. So, I'm speaking, I suppose, wearing more than one hat. So, as Ram knows, because Ram and I have had conversations about this, my company straddles more than one area of the infrastructure. So, we're primarily a hosting provider. We are a DNS provider. We are also a fiber ISP. We provide connectivity, and we do public cloud, and we do private cloud. We do a lot of different things within the ecosystem.

And I think having conversations about this is really, really important because it's very easy for people to look at the shiny object. Oh, AI is wonderful. It's going to solve the world's problems. Putting stuff in the cloud somehow makes it super-duper resilient. No, it doesn't. The cloud is just somebody else's

computer. I mean, that's the reality. And we've seen, as several people have mentioned, cascading issues over the last while.

And the concern I have was when you look at new entrants into this space, be they registry operators or registrars, there is a degree of naivety with some of these people that they may think that they can rely solely on these technologies to solve problems when they haven't actually dealt with actual basics.

I mean, things that are within the remit of ICANN is that there's, I think, as Suzanne says, obviously, you don't want to get to scope creep, and you don't want it to be solve all of the security issues through ICANN. That would be wholly and massively inappropriate. But it's broader than the IANA. Because you can't, on the one hand, say, oh, under the registry contract, you need to do this, this, this, and this, while actually ignoring the flames over here in the corner. I mean, that would just, to me, just makes no sense.

So, I think there definitely should be a space to have some of these conversations. I mean, it's like SSAC, the first SSAC meeting I came to about 19 years ago, somebody was giving a presentation about IPv6 support on routers and in people's homes and things like that, and how the devices at the time simply did not support it.

So, you could talk about, let's spread the IPv6 love, but nobody could use the damn technology. And that's an important bit of information to have. Thanks.

RAM MOHAN Thank you, Michele. Other comments? You're all very quiet here today. Beth?

BETH BACON We just had a lot of fun before you got here, and then just tired ourselves out. So, I think, so this is Beth Bacon. I think that this, I mean, we have these conversations about the baseline of the safety and operation of the DNS, and I think that's very important. I wouldn't hazard to discuss, to share a registry-based opinion, but I'm very happy to just take this back and keep it in mind as you guys noodle on it.

I think this is the technical term, and think about this as an issue to discuss going forward. I do very much appreciate the comments around scope and mission. ICANN has a very specific mission. We have very narrow kind of impact on our various infrastructures that we operate. So, I think that's important, but certainly some coordination is not out of line. Thanks.

RAM MOHAN Great. Thank you. More to come. I mean, from our point of view, this is the opening of the conversation, and we would really like to have you continue to bring your thoughts to us. Okay. So, there's no real takeaway action, please do this, please do that, other than let's continue having an open conversation on this topic. All right. Next slide, please. Okay. Beth.

BETH BACON

This is Beth Bacon. We had our meeting in Dublin, and we had floated the concept that with the Code of Conduct on SOIs being now in place, the registries are, and I keep saying somewhat selfishly, because I don't want anyone to complain to me, and I don't have a process, because that sounds terrible.

So, we as registries have been thinking about how to operationalize that internally, have a process for how we take in and address and escalate any sort of complaints. However, that might work between if it's not a registry-to-registry concern, but a registry to SSAC, because you're trouble. Why wouldn't we? So, registry to SSAC, or if we had, if SSAC had a question about a registry participant, then I think we just want to be able to navigate that in a predictable way.

We are still working through what that should look like for the registries, but just curious if you are also thinking about that. There is some guidance provided in the back for enforcement in the appendix of the Code of Conduct. It's fairly light and principles-based, which is helpful, but it does kind of very clearly push the responsibility to navigate these to the community. It's not like we're going to send it to ICANN, and they're going to make a decision. So, just interested in if you folks have been noodling on that at all.

RAM MOHAN

I think from a principles point of view, we're strongly aligned with transparency is important. You got to know where people are coming from, and inside of the SSAC itself, it's less about conflict, because if you were accusing people based on conflict, then we'd have almost nobody doing work inside the SSAC, right? Because everybody comes with a great deal of knowledge and experience and expertise, but Billy's with the registrar, and I'm with the registry, and so on and so forth, right?

But what we insist on is disclosing what your interests are and being very transparent about it, and we impose a very strong requirement on our members that as soon as you have a change, you have a responsibility to update it.

This is not a, oh, once a year please go and look at it. It's not just, at least from my point of view, it's not just what is the code of conduct, what is appropriate, but it's also what is the baseline that builds trust, and if you don't know where the heck the other person's coming from and what their motivations might be, it doesn't mean you will ignore what they're saying, but at least it'll be a part of your thinking that says, oh maybe there is a particular point of view, right?

So, we're strongly aligned with where you are on this, and inside the SSAC, we encourage people to come in with a very defined point of view, so long as there is also clarity as to what their own allegiances might be or where they're not so much where they're coming from, but knowledge of who is paying the freight.

BETH BACON I don't see any other hands. I appreciate that. I think we're just trying to keep the conversation going and encouraging transparency. I know that several of the specific implementation items are GNSO-based, but I think it is a community code of conduct, and that's why, so just wanted to, interested in keeping the conversation on transparency going, so appreciate that. Next.

RAM MOHAN Next slide, please. I'm sorry. Yeah, I think it's on us, but I'm wondering if --

BETH BACON Thers is another slide.

RAM MOHAN Oh, there is a slide after this. I was hoping we'd get to the next slide. There we go. There we go. Yeah, I wasn't just going to riff on it, you know. We actually prepped for this session.

So, we wanted to share with you something that the SSAC is doing. You know, a couple of years ago, the SSAC began working with the ALAC on a series that we call Safer Cyber that was focused on -- we have content, we have expertise, we have knowledge. How do we take that content and provide it to other folks in our community who have the ability to distribute it in their own way uniquely?

So, we started doing that with the ALAC. We did a program with them on credential management and phishing, and we provided the base content. They converted that into beautiful graphics and things that were digestible to a regular person and had basically no jargon associated with it, right?

Now, this year, we're moving along that line where we've announced and we've just begun collaboration with the ISP CP, and I won't read through everything that's here, but you'll see that at each of the ICANN meetings, we're committing to providing some of our experts to come and speak to specific topics, but the other ones, the intra-sessional meetings, our webinars were, again, we'll have our experts come and provide informational content that, again, is intended to elevate the amount of information that's there, knowledge, and in some cases, bust some myths that might be there, right?

So, that's FYI better know when we were talking earlier in prior sessions about, hey, how can we guys collaborate, and I thought it might be interesting to just share this with you as a conversation starter. I'll pause for a moment to see if there are any thoughts or comments.

SARAH WYLD Hi, this is Sarah from the registrars. This looks great. I love a training series. I love learning about security. I am most certainly

going to attend the Privacy versus Security at ICANN86. Can't we have both? Thank you.

RAM MOHAN Please, Tara.

TARA WHALEN Yeah, I'm expecting to be the one running that session. It's Tara Whalen from SSAC. So, also, I'm happy to hear about things you might want to know about. So, if you want to drop me a line or connect with me because we're helping in designing a session, I'm always happy to talk about privacy. So, thanks.

RAM MOHAN Thanks. Michele.

MICHELE NEYLON Yeah, thanks, Michele, for the record. Look, I think training and capacity building is always welcome. The responsible DNS blocking implementation depends how you're going to frame that, because I can see that getting, raising the hackles of some stakeholders.

I'm not suggesting there's anything wrong with what you're going to be doing. I was at the last session where you gave the kind of overview, but coming away from that, several people that I spoke to got an impression of it, which was definitely not what was intended. So, I think with that one in particular, there is a kind of

degree of finessing and nuance that is required, because otherwise a potentially useful and good thing could end up just blowing up and not being that at all.

I do like rooting security. Strong believer in it. Love that. Hopefully, you can get the right people, though, in the room who can actually learn from that. Thanks.

RAM MOHAN: Thank you. And Danielle, can we please take an action to connect with Michele on before we get to responsible DNS blocking implementation, if we can pass slides past you to just see if we've got the right tone or the right level of nuance. I mean, the slides are going to be some variation of slides that we've already done in public.

MICHELE NEYLON: Thanks for that. Look, I'm always more than happy to look at things and all that, but I'm not the person you need to convince.

RAM MOHAN: Understood, but you have the eye on it.

MICHELE NEYLON: No, that's fine. Just as long as you understand, I can try to channel my inner name of various people here who I won't name, but even when I try my best to channel them, I may not succeed, but I might

be able to spot a very obvious red flag. So, I would suggest engaging just with certain people. We can discuss that offline.

RAM MOHAN You got it.

MICHELE NEYLON Okay.

RAM MOHAN Thank you. Next slide. Oh, Beth.

BETH BACON Thanks. This is Beth Beacon. As you go through and do those sessions, I assume they're kind of scheduling them in the SSAC room in your own time, if there are ways that we can help cross-promote that, because I think it's things that, there are things that, how do I say this?

People don't always look at the schedule for the SSAC, just because they're like, oh, no, it's confusing. I'm afraid of them. They're so smart. What are they talking about? So, I think if there are things that we, ways that we can identify these kinds of as approachable and informational, if there's something that we can do with the registries, very happy to help with that.

RAM MOHAN

That's a great point. These are not our sessions. These are ISPCP sessions, hosted and run by the ISPCP, just as the safer cyber ones were ALAC sessions run and hosted by the ALAC. We simply happen to be in the room providing kind of the anchor content on it, right? So, that's kind of what we're doing, but we'll still take you up on your offer of collaboration. Thank you.

All right. I'm going to do a quick update for all of you. There's some work that the SSAC is doing. These are Work Parties, and I wanted to make sure that you get a quick picture of what we're doing.

So, first, we've been working for almost a year now on what are the practical guides and practical issues if you wanted to implement DNSSEC, right? So, this is not a cheerleader document that says it's the absolute best thing. Close your eyes and just implement it, and all will be well, right? This is a document where we're saying, hey, evaluate tools. What are the trends? What are the barriers to implementation? What are real-life issues that have happened, right?

There have been outages that have been linked directly to DNSSEC implementation, for instance. So, we're looking to make sure that we can express in our document what the practical tradeoffs are, what lessons have been learned, and potentially what actionable solutions, what are implementation steps that could be taken.

Now, what we've done is we've interviewed several ccTLD registries that have implemented DNSSEC and that have had experiences,

operational experience with the deployment of DNSSEC, and this is kind of early insights of what we've seen.

They've said that the most important expense is not the technology expense. It's the teaching people what the heck it is and how do you keep once you sign it, how do you make sure that it you have somebody who knows how to roll it and roll it well, and those kinds of things.

So, there's the largest and most important expense is that. Tooling and automation is an issue, and registries that have implemented good amount of tooling, it has resulted in their implementation and the adoption of DNSSEC quite seamless.

Interestingly and surprisingly, they've said the extra investment, hard dollars, if you will, is not very high. It's a minimal one-time cost on it, and that a lot of the implementation success is dependent upon registrar support, support from the registry for registrars, support from registrars to their end users, et cetera, right? So, that's the early insights from there.

We want to hear from you in the G space, and we would like to find out from you what does adoption of DNSSEC look like? Doubtless some of you have looked at DNSSEC and said, this is not for me, and doubtless some of you have looked at DNSSEC and said, of course, we have to deploy it, we want to do this, right? We would like to understand what motivates or delays DNSSEC adoption decisions? What does it cost to deploy and sustain DNSSEC in your environments? And we would dearly like to hear about

deployment experiences, as well as what hurdles remain in promoting DNSSEC across the ecosystem. So, we really want for your input to us.

So, if there are people who are willing and interested in speaking, not just positive experiences, but not so positive experiences as well, either raise your hands here in the room, or please come and write me. I'm one of the co-chairs of this Work Party, but we would really like to engage with you and better know if you could help with the gathering of, or really both sharing that request from DNSSEC into the CPH, as well as soliciting, helping people write back to us and saying I put my hand up to contribute. That would be really appreciated.

BETH BACON Sure, feel free to, when you want feedback, send us a message in an email, and we will forward it, and hopefully we can arrange some good back and forth.

RAM MOHAN Lovely. Thank you. Next is another Work Party, which is focused on the responsible integration into the DNS ecosystem, and I believe the chair of that Work Party is in the room. So, shall I hand it to you to just briefly talk about this, Rick?

RICK WILHELM Sure. Thanks. Rick Wilhelm, this responsible integration has been, we've been working for a while. What it says up on the slide, which

I won't read, is all good and well. We've got pretty good participation inside the SSAC on this. We've got some registrar involvement, too. Jothan is involved. I didn't see Jothan in the room. Maybe he had to go. I heard him. Oh, he's all the way, literally, back benching.

And then, one of our invited guests is Tom Barrett, who a bunch of people here know. I didn't see Tom either. So, we've been working on this. We've been interviewing folks. Our goal is not to give advice to the blockchain folks, but, because they have no real interest in listening to the SSAC, for obvious reasons.

We're really, our aim is to develop findings and recommendations that are interesting and useful to registries and registrars to say, if you're going to be operating an ICANN TLD and doing stuff with your TLD in which your names, in which you're going to be taking part in activities which involve integrating your names with a blockchain, here are some things that you need to help remember in order to avoid things ending in sadness and tears, as I've said in the Work Party meetings.

Yeah, either literally or metaphorically. And we see, you can see some of those things over on the right side of the paper, or the right side of the slide, which are some examples that could result in sadness and tears. That's about it for now. Thanks. Happy to take questions.

RAM MOHAN

Any questions for Rick? Okay. Let's go to the next slide. The slide, ignore everything on this slide except the title. Okay. So, here is what we're trying to do. Gautam, do you want to speak to this?

GAUTAM AKIWATE

So, the idea behind DNS transparency was, it was motivated by a bunch of academic work which showed the rise of really sophisticated threat actors, especially nation state actors, that were targeting DNS infrastructure, and especially registries and registrars, where they would come in and sort of swap out the DNS names, the DNS configuration, and sort of get DLS certificates and sort of pretend to be government organizations, infrastructure providers, and sort of use that as a vehicle to get inside these organizations.

And part of the goal of this Work Party is sort of an exploratory, it's exploratory in that we want to sort of get inspired from the certificate transparency work and see, is there a notion of DNS transparency that we can sort of build on? DNS nominally is all open, but it's not really unless you query every second, every millisecond, and these threads that we're seeing are operating at a super-fast scale.

So, part of this is asking the question, can we sort of take a page of certificate transparency and bring that to DNS? What would that look like? And what are the kind of attacks that it would prevent? And what would that mean for the DNS ecosystem?

RAM MOHAN Thanks, Gautam. And there is a CZDS connection there, right?

GAUTAM AKIWATE So, I think part of what we are trying to explore is thread actors know that CZDS is published once a day, and they are sort of taking advantage of the time in between and sort of launching their attacks at that point of time. So, I think Matt had brought this up. Essentially, are there improvements we can make to CZDS, enhancements that we can sort of make to existing processes so that would uncover these attacks?

RAM MOHAN Any questions on this? This is early work, but we think this is, I mean, this area, there are real exploits happening. There are real problems. The security research that we're seeing shows real issues happening. I mean, I was struck on the CZDS side, I was struck by some of the comments that said thread actors are registering names, are doing things, doing bad things with those names, and then they're deleting the names within the 24-hour time period.

So, it doesn't show up in the CZDS. So, harm's been done, but it's kind of invisible, right? That was my interpretation of what I heard, and that really got my attention because I was like, wow, these are ghost domains. There's real harm, but you can't actually see them

if you want to research them. So, that was interesting for me. I got that right, the characterization right, right, Gautam?

MICHELE NEYLON

Okay, yeah, thanks Ram. It's Michele. The deletion of the domain name within the 24-hour period, that's piqued a little bit of curiosity from a couple of us over here, because from a technical perspective, it'd be quite hard for a registrant to do that with most of us. Like, I can tell you categorically, my registrants can't do it. A lot of registrars don't enable that facility either. I mean, you'd have to go off and hurt some small animals to get us to actually delete a domain just like that. And we also have a lot of limits around what we can do in the gTLD space with the AGP limits and everything else.

So, if it's happening in gTLDs at any scale, I mean, if it's only one or two domains, I mean, who cares? Because that's not something that's statistically interesting. But if it's happening at scale, then that suggests to me that there's a problem inside the house, and it would be good to know a bit more about that, because as I say, most registrars would not enable that kind of activity.

So, I think it'd be interesting to see more on it. Is this solely gTLDs? Are you also looking at ccTLDs? And again, the same thing, because most of us don't allow the registrant to do this, and definitely not at scale. So, it would have to be done by the registrar or the registry.

GAUTAM AKIWATE

Right. So, this is some academic work that is done by a relatively new SSAC member, Rafaele, back when I was in academia. So, basically, the insight that Rafaele had and we had was if you look at certificate transparency logs and domain gets a certificate issued for them, that is a sign that that domain is alive and kicking. And when you don't see that domain show up in CZDS at either point of time, that is a domain that sort of disappeared within the 24 hours.

So, it was, you can go to it, and there are many valid reasons why that domain might have been deleted. It could have been abusive. So, there are a lot of legitimate reasons why it could have been deleted, but we see that this is not a small problem. There are lots of domains. I can point you to a paper. So, this is published research. So, yeah.

MICHELE NEYLON

I mean, please do, because the -- sorry, it's Michele again. It's just because from our perspective as a registrar, it's for us to delete a domain, it's quite manual. I mean, I do have interfaces over things and all that, it's the registries delete domains, sure. But even so, it's just trying to understand what's happening.

JOHN LEVINE

Yeah. This is John Levine, if I can butt in a little bit. If we could, if we, for some version of we, could simply get a close to real time

feed of these are the new domains to feed to the sorts of people who do phishing and malware detection, we could put them on blacklist, even if you don't, even if you don't delete them.

Yeah. Because yeah, the cycle is like domain is created at time zero, bad stuff happens at time one beats from time one to time 23. And then by time 24, it's gone but, but, but, but by the time we can see it in CZDS, it's too late for us to do anything about it.

RAM MOHAN

So, action out of this from the SSAC Danielle is we'll provide a link to the report. We'll share that with you. But we want, again, we wanted to highlight it to you because what we're seeing inside, I mean, from the security researchers' point of view, this is not an isolated onesie twosie thing. It's being the paper says it's at scale.

Okay. So, more work to be done, but just wanted to give you the heads up that that's working on a, on a, on a paper on this area to, to write something about it and to expose this, but we, we don't want to expose this as a full scale paper before all of you who actually get to operationally touch it, get to know about it and get to do something about it. If there is actually a problem that you can touch, right. So, we'll get to that point in just a little bit. Michele and then Rick.

MICHELE NEYLON

Yeah. Thanks Michele again. Look, I think we could easily get into the weeds here, which is probably not particularly productive right now. I think something like this is definitely a topic.

Personally, I'd be interested in just reviewing the actual paper to see what they're saying and how they're saying it. Because I've heard a couple of different things from a couple of different people and one or two of them make perfect sense to me from a technical perspective. The others definitely don't make sense to me because as I say, the, the level of access you need to be able to do that at the speed is what I'm kind of having difficulty with.

So, I'll have a look at that, not disagreeing with you, John, I just need to see what the research actually says and then I can have better clarity about what it is or isn't. I mean, I think from the perspective of the registrar, some of the things we've been talking about in other fora is around some of the farcical limits that ICANN is imposing on contracted parties, which is hindering our ability to mitigate various forms of abuse, be that technical abuse or other forms of abuse.

And this is me speaking on behalf of myself and not on behalf of anybody else. I find it absolutely bonkers that I am penalized for deleting domain names that I know have been paid for fraudulently, but I'm penalized. And if the registry operator tries to help us in inverted commas, they will be in breach of contract. That is bonkers. And that to me is something which is a hell of a lot easier for a lot of us to be supportive of in addressing than some of these

kinds of weird ass edge case scenarios that certain people raise in various fora. Thanks.

RAM MOHAN Amen. You know we're not keen on edge case “threats”. Rick?

RICK WILHELM Just briefly. I won't comment on Michele's comment. I just wanted to offer that there's, there's a variety of opinions inside the SSAC about this topic. Thank you.

RAM MOHAN What will happen is eventually the variety of opinions will end up expressed either as some kind of consensus in the document or the document will not even get to see the light of day, something like that will happen. So there's on almost every Work Party that we work on, there is a pretty robust engagement and interaction inside the SSAC. Gautam.

GAUTAM AKIWATE Yeah. I just wanted to say what we did, like it's basically empirical research. Like every time I've been told, oh, like this cannot happen. And I think Jim has been the victim of me harassing him saying, oh, like, this is what I see. And he was like, oh, maybe not. And Joe Avley too. And then we go in and he's like, oh, like there is this corner case in which these things happen.

So, I think those are the kind of scenarios that we are interested in, like how threat actors sort of take advantage of this. And it would be great to know that, oh, like this is just an exception or maybe there is only a small thing that we need to fix to address the issue. But this is empirical data. So, we have this data. So, let's try and make sense of it. And let's try and figure out like why this is happening. And maybe there are legitimate explanations for what's happening. But the fact of the matter is like we see this data and we see real world evidence of things happening. So, let's try and figure out why that is. And so, it would be great to have a conversation around that.

RAM MOHAN

Thank you, Gautam. Our last slide is a Work Party that we have also begun. This is on DNS Abuse and AI. And again, you can ignore all the content of the slide and we'll talk to what we're actually doing. This is very early stages yet inside the SSAC. We're still at the point of scoping what this topic actually means and what do we have meaningful and useful to say.

The preliminary discussions that we've had inside the SSAC has been that it seems like at this point, the advent of AI and the various pieces associated with it doesn't seem to have created new threat vectors yet. What it seems to have actually created, what's pretty evident is that the scale and the speed and the sophistication and the learning and the sophistication of the well-known existing

attacks, we're seeing a great increase in scale, speed, sophistication.

So, that's been the preliminary discussion. So, we're not at this point in our Work Party, we're not at the point of saying, AI is here, the sky is going to fall, but we're in the thing of better watch out because this thing is moving seriously fast and the scale is not just a standard scale, this is moving at a really rapid clip. So, that's kind of where we're at. Jeff?

JEFF BEDSER I'm just going to say may or may not fall for the sky.

RAM MOHAN Okay.

MICHELE NEYLON Yeah, thanks, Ram. It's Michele again. Look, I think this is a really interesting topic simply because it's got AI in there, so that must make it cool. Right? I mean, you remember back 10, 15 years ago, you put cloud on a slide and that got you those extra points and that got you the investment. Now you shove AI into anything and that's going to get you the brownie points.

Jokes aside, yeah, it is something that I think we all need to be conscious of. I'm not sure what we're meant to do with it though. That's the kind of thing is like, I see discussions happening in various fora where there are people talking about generating

100,000 pages of content in 20 minutes, not for nefarious purposes, unless you consider late-stage capitalism to be nefarious, which is debatable.

But obviously, threat actors, scumbags, which is my preferred term for them, when I'm at a microphone, I use other words when I'm not on a microphone, they will use the same technology that I'm using to help cat herd my calendar to also impersonate me in emails to my CFO, which I thought was really, really clever, by the way, they're not sending them invoices with an entire thread of emails I apparently had between them and me.

What can we do? I mean, I think that's the question that I don't know what the answer to is. I mean, is there anything we can do, or are we just simply recognizing the fact that AI means that they can do this stuff a lot faster? And also, why didn't we all buy shares on Nvidia? Thanks.

RAM MOHAN Thanks. Jeff?

JEFF BEDSER So, I think that there's two directions, probably more, but let's go with the two primary directions for this Work Party. One is an advisory that says, be aware of this scaling issue, and it needs to be addressed. But it's also possible the expertise that we're bringing in both within SSAC and externally, that maybe the answer is practical applications of AI to fight AI.

You know, because basically, we are in an escalating weapons war. And if we don't do the scaling appropriately, it becomes the point where the fraud volume gets to a point where it's not human attainable levels that we can't deal with it.

So, I think that that's also part of the discussions in the Work Party. The bigger problem, of course, is this is really nascent, as far as people studying it, it's moving faster than the people are studying the problem. So, we understand that we need to at least get to the point where we can advise the community and the Board about how this can impact the DNS and the DNS, particularly around DNS Abuse, where the volumes really are kicking up at levels that are just really hard to believe.

So, hopefully, we'll give you something more than a yes, the sky is falling. And you should know that as you're building your shelter.

RAM MOHAN I see the beginnings of a comment there. You might as well get it out.

MICHELE NEYLON Thanks. There are other people in the queues, which I didn't want to preempt anything or respond. I'm not sure why you're fixated with me building a shelter. Personally, I was just going to buy myself a few cases of whiskey and just go hide somewhere. Automation around certain things is always really interesting. And I'm sure we all like to leverage as best we can. But as a registrar,

and as a business, I need to make sure that I can actually check things.

And I don't see automation as being the key to everything. So, I'm not quite sure how we're going to deal with this apart from being able to leverage some of the tech in some parts of this. I would never feel comfortable with anybody saying that we're going to be able to mitigate it in an automated fashion, though.

RAM MOHAN Thank you. Sarah?

SARAH WYLD Hi, this is Sarah. AI is not my favorite topic. I appreciate the comment that AI is not making new problems, but rather making current problems faster. I do sort of wonder, like, what AI are we talking about? Are we talking about LLMs? Are we talking about something different? And then I also wonder, just going back to the resilience topic, one thing I think about when AI comes up is the huge power draw, electricity, I mean. And so, I wonder if that's something that the SSAC also thinks about. Thank you.

RAM MOHAN I'll cover that last part. That's the reason why we think we need to start having a discussion about resilience. There's the environmental factor, there's other pieces of it, not just keeping the lights on. So, but we haven't talked about that inside of the DNS

Abuse and AI piece. Jeff wants to venture a response to the first part.

JEFF BEDSER: You're not the only person wondering whether we should define or how we should define or how we should describe AI. That's also a topic within the Work Party.

RAM MOHAN: Ashley?

ASHLEY HEINEMAN: Hi, everybody. Ashley with GoDaddy. Oh, and I can't see with my glasses on. I won't proselytize too much because I am not an expert. I'm not a security expert, not an AI expert. But kind of jumping on Sarah's coattails, there's so many different aspects of AI and so many different ways it can be used. So, it's hard to avoid the sky is falling.

So, if we can get to a point where we can be more specific, I think that would be helpful. I say that not really knowing how to achieve it. But also, I think it's just a reality at this point. I think there's still a lot of naysayers about AI, but I think this thing is here to stay, guys. And it's just a matter of how do we keep up with the speed?

And I think also finding ways that we can benefit ourselves from the technology, whether it's, I mean, I'm not saying that necessarily is building, like relying on AI to fix the problems for us. And you guys

already heard me say this in our session with the Board, looking at protocols coming out of the IETF that could help us, whether we decide to go down this path or not, but leveraging the DNS as a vehicle, as infrastructure to deal with agents, to be able to locate agents, but also use SSL certificates to also build some trust into that process.

And I think there's ways that we can look at this as the big, nasty thing that's going to swallow us all up. But I think there's also other opportunities to, how can we embrace this in a way that actually brings some sanity into the space? Thanks.

RAM MOHAN

Thank you, Ashley. I think that's exactly on point. You know, in the SSAC, AI is one topic, but we look at the reality that the namespace, as we know it, continues to evolve. And as it evolves, often it seems like they begin as separate and distinct from the ICANN remit. Then at some point they seek to integrate or intersect with the DNS resolution space, right?

So, we have agents, there's reports that there might be billions of agents or whatever that might leverage the DNS. And there might be a scale issue, there might be transparency, discoverability, there's a whole lot of things to go and look at in that area. And we haven't fully got to the point of precisely what is the scope of what we're looking at and what do you want to respond to.

We're constraining ourselves to the abuse area, right, rather than general purpose capacity or general purpose, other issues that you hear about in the wild. So, that gives you a sense of the things that are on the SSAC's, not just mind, but actual on our ticket, what we're working on. And with that, I'll hand it back to you, Beth.

BETH BACON

Well, thank you very much. I won't kind of go on and on because we only have about 30 seconds. Other than making me feel like I need to go buy a generator and some dried food, I generally like having this meeting with you guys. A little bit nervous now, but really appreciate the exchange.

You guys are, I think, it's nice that one of the things you do is you talk about a lot of issues and sometimes you're like, never mind, we don't agree. Turns out it's not a thing. But it's always really nice to hear the depth and breadth of what you're discussing and sharing that with us.

So again, if you have things that you're looking for input on, just flag it for us and we're happy to pass that on and work out some chitchats. Thanks. Owen, anything?

OWEN SMIGELSKI

Nothing else to add. Thanks, everyone.

RAM MOHAN

Thank you.

NIKKI SCHULER We can end the recording. Thank you.

[END OF TRANSCRIPTION]