ICANN86 Seville | PF – RSSAC: SSAC Community Open Mic
Thursday, June 11, 2026 – 14:45 to 16:00 CEST

KATHY SCHNITT: Thank you, Nick. Hello, and welcome to the RSSAC/SSAC Community Open Mic. My name is Kathy, and I'm the participation manager for this session. Please be advised that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. This session is designed for community engagement. To ensure we hear from everyone, remote participants, please join the speaking queue by using the raise hand feature in Zoom. In-room participants, you may use your hand in Zoom. We will also have a roaming microphone available. Please raise your hand in Zoom and a staff member will bring the mic to you. Before speaking, please state your name and affiliation for the record. While you're welcome to use the Zoom chat for discussion, please note that the comments or questions posted in the chat will not be read aloud. All formal input should be shared via the speaking queue. With that, I'm happy to hand the floor over to Ram Mohan.

RAM MOHAN: Thank you, and welcome to the Open Mic. To my left is Jeff Osborn from the RSSAC, and we're going to jointly help manage this

session. On the next slide, you will see what our agenda is. So we're going to spend a few minutes just introducing you to the SSAC and to the RSSAC, and then we switch straight to you, the community, and it is an opportunity for you to ask us anything. We don't promise to answer everything, but you can ask us anything. So on to the next slide.

Let's start with an overview of the SSAC. Again, I'm Ram, I'm the chair of the SSAC. The SSAC's role is derived from ICANN's mission to ensure the stable and secure operation of the Internet's unique identifier systems. If you go back to why the SSAC was formed and when it was formed, we began informally in 2001, right after the events of 9/11. A bunch of us got together and we said, "Well, if people could go and take down big buildings and cause devastation in that way, what would happen if they targeted the Internet or pieces of the critical infrastructure of the Internet, and who is there to watch or to look at that?" So that was the impetus to get the SSAC started. We met informally for the first time at a meeting in LA in November of 2001, and then we were formally chartered in 2002. Next slide, please.

So we have a few responsibilities. We engage with the Internet technical community and key DNS infrastructure operators. We analyze risks and threats to the Internet's naming and address allocation services. We coordinate with the entities responsible for the Internet's naming and address allocation security, and that coordination typically comes in the form of our members engaging and directly participating in many of the standards and other

bodies that are involved in this work. We then inform the ICANN Board about our activities. We provide reports and recommendations to the community and to the Board, and our recommendations, we strive quite hard for our recommendations to be grounded in security assessments and operational insights. Rarely do you find the SSAC coming in on policy or pure policy-oriented matters. Even when there are policy-oriented questions, our approach is to bring the security and stability perspective on it. A case in point is the current policy development process that is underway, the PDP-1 on DNS abuse and associated domain checks. And we have SSAC members who are participating in that PDP, and their perspective is to inform and to provide the security and stability angle to that. Next slide, please.

This is a quick look at who we are. About 23 members of the SSAC are in North America. We have two members in Africa, four from Asia, Pacific, and Australia, and we have 11 members from Europe. Sadly, we are still at no members from the Latin American Caribbean Islands region, and we encourage people who are interested and who might be qualified to become a member of the SSAC to apply. There is a specific process to apply. You can find that on the SSAC's webpage. And to my right here is Tara Whalen, and she is the chair of the membership committee. And if you are here in the room, come and talk to her after the session or ask questions here about what does it take to become a member, how do you go through the process. We're happy to answer those questions as well.

The leadership team on the next slide, there's a really great set of people. Tara to my right, Jim Galvin to her right, is the liaison to the ICANN Board, Jeffrey Bedser and Barry Leiba. Barry is somewhere in the back. Yeah, there he is. He's got his hand raised. Barry is one of the members of the leadership team, and Jeff is-- I don't see him here. But these are from the SSAC members' side. But the way we run the SSAC is that the leadership team actually consists of us as well as all of the amazing policy support staff who are part of the team, Carlos Reyes and Danielle Rutherford and Kathy Schnitt. Kathy is right there in the back. You can see her raising her hand. Dan is here. He is also super important for what we do, and Michael Puckett. So together, that forms the team that helps the SSAC run and do all the things that it needs to do.

Now, briefly to the key topics on the next slide, the key topics that the SSAC keeps a constant eye on and is consistently engaged and focused on. We have five keystone areas: DNS abuse, new gTLDs, DNSSEC, alternative namespaces, and Internet governance, the security, stability, and resilience aspects of Internet governance. So those are the five areas where we have a keen and strong, continued work that we work on. On the next slide, you'll get just a quick look at significant SSAC publications over the, I guess, 25 years almost of our existence. And there's over 130 documents that we have published. They're all on the SSAC website. They're all accessible. And many of these documents, we not only have the full documents, which are multi-page documents, but we also have 500-word executive summaries as separate documents that are

written in easy-to-understand language that makes it digestible. So if you or if organizations or others who would find these things important or useful, take those documents and share it, share it with policymakers or others who are not technical, because those documents are written to take technical topics and make them accessible to a non-technical audience.

On the next slide, it gives you a sense of our recent publications. We've written recently about the fact that the Domain Name System, the DNS, runs on free and open-source software. So we have an entire document written on it. We've also commented about the functional model for the root server system governance. We've written about, and we've provided guidance, and this was a major amount of work and a significant number of years that we spent on providing guidance and guidelines for how to manage name collisions. And much of that work is baked into the risk management of this new round that is currently underway that ICANN is managing. And we are also very active in the domain name registration data accuracy. We have members who are participating in the SSAD work. We have work parties currently on the responsible integration of other naming systems into the DNS ecosystem, and that's really aimed at technologies in the blockchain space that desire to integrate into the DNS ecosystem. The chair of that work party is here, Rick Wesson, right there in the back. Please raise your hand.

And we also have work that is coming to a close on what are the operational considerations if you want to deploy DNSSEC. So we

are working on a paper on that. I'm one of the co-chairs of that work party. We have a work party on DNS abuse and AI, and I don't know if the-- yeah, the chair of that work party is just standing up there, Laurin Weissinger. He is one of the co-chairs of that work party. And we also have a work party on DNS transparency, and that has two co-chairs, and I don't know if they're here in the room, but we do have them here in the room. So those are four work parties that we're working on. We also have, we're trying for the first time, a research apprentice, Gustavo. I don't know if Gustavo is-- oh, there you are. Gustavo is our research apprentice, and we're trying to try that as a way to get people who are relatively early in their careers to engage with the work that the SSAC does.

Now, at this ICANN meeting, the SSAC partnered with the Business Constituency, and on Monday, we were able to host a plenary session on the potential incoming impacts of AI on DNS abuse. And that was a well-attended session. And I wanted to share with you some of the-- so we asked a bunch of questions to the audience, and we asked the audience what they thought of several topics. So I'll just wait for the slide to come up. I wanted to share with you what those responses look like. So we asked a question, how well do you understand the impact of AI on DNS? And you see a majority of the room considered that that's already an operational concern. The next question that we asked was about which aspect of AI-driven DNS abuse concerns you most. And we had many people talking about or concerned about more sophisticated and convincing phishing attacks, as well as the increased speed and

scale of abuse campaigns. The next slide, we asked them also about whether they believe that the current DNS abuse mitigation mechanisms are capable of operating effectively against machine-speed AI-assisted attacks. And you see a plurality of opinion, 44% saying, "Yeah, it's there. It just needs a little bit of upgrade, or some more work." And another set of folks saying, "No, it's not enough. The current mitigation methods are human-paced, and it needs to be not just tweaked, but it may need something more significant than that." The next question that we asked was about how ICANN should fulfill its DNS stewardship role, and the vast majority of the responses spoke to ICANN needing to understand the technology and to monitor its use rather than just jump just at breakneck pace into trying to deploy something. So understand the problem space before you start thinking about what to do. And the final question that we asked was, what role should the community play in addressing this? And it was interesting, 38% said, "Should support development of technical mitigation frameworks," and 28% said, "Expand policy expectations around DNS abuse responses." So I thought these were interesting responses from the audience on this topic. Our intent in hosting it was not to actually drive any policy outcomes. It was to just begin the awareness and to also ensure that the community recognizes that we are watching this space, and we are paying attention to the space, but it's too early to start to think about what specific policy-oriented measures or even technical-oriented measures need to be done. So those really

give you a sense of what the SSAC is about and what the SSAC has done. And with that, I'll hand it over to my co-host, Jeff Osborn.

JEFF OSBORN

Thanks, Ram. Yeah, I attended that session, the AI questions, and it was interesting, and I was mostly surprised and pleased with the answers, too. So that was a really positive thing. Let's see. We have another deck to switch to, which I suppose is in process. Yes, it is. Next slide.

RSSAC. RSSAC is-- everybody thinks they're unique. So RSSAC, I think, is unique among the SOs and ACs at ICANN in that we have a really, really narrow scope. We're basically involved with the Root Server System, and we advise the community and the Board on matters relating to its operation, administration, security, and integrity, and that is it. I think the SSAC can be seen to have a remarkably wide remit. Ours is rather narrow. Next.

We are made up of a committee that produces advice mostly to the Board, but also to other ICANN bodies involved in the DNS. The root server operators are represented inside the RSSAC, but RSSAC doesn't involve itself in operational matters. RSSAC is made up of primary and secondary representatives from each of the root server operators. There are 12 operators, so doing the simple math, there are a total of 24 members from the operators, and then incoming liaisons from other bodies. So in total, there are 28 members. Next slide.

The RSSAC Caucus is a broader body than the 28 members of RSSAC itself and adds about 100 DNS experts to the group. They have all made public statements of interest, and they get public credit for-- we're learning to speak English on a microphone. Public credit for individual work. The purpose is to have a group of DNS experts who bring expertise to publications, and so that we are transparent and have a framework for how to finish things. We were just noting the other day, almost all of the work that's been done by RSSAC, either currently or recently, is done by the Caucus. Seven years ago, all of the work was done by RSSAC. It's been a process moving it over, and we are most of the way there. Next slide.

Here's some of our recent publications. You can always cheat and guess how many publications we've put out because there's a number there. So 63 means we've put out five dozen and change of these. These are some recent ones. How to change IP addresses is particularly sticky with changing numbers for a root server system, but we have that documented now. We've been doing work on security incident reporting, because doesn't everyone? And then there has been a lot of work that is currently out of our hands involving further changes to the governance system of the Root Server System, which I think is of interest to a lot of folks. And then we've just wrapped up a couple of work parties on the basis of what is the Root Server System, how does it work, and how does it measure things, 001 and 002, and those will actually be published in their newest versions, I think version 3 and version 10, in the

coming weeks. We like to talk about anything, mostly about the DNS Root Server System. So if you have questions, we're going to be approaching that part here. Our metrics, how it works, who can join, those are all interesting questions we find. And next.

I have a beard in this picture, and I'd like to thank Barry for that, because the last time Ram and I got together, he raised his hand and said, "You had a beard in the picture. Why don't you have a beard?" So I grew this for you, Barry. I hope you appreciate it. Hans Petter, whose day job is the president of the RIPE NCC, is co-chair. In my day job, I'm the president of ISC. Hans Petter's organization obviously runs RIPE, the Atlas network, and all kinds of things like that. And he is on the call. Is that what you were pointing at? On the call.

HANS PETTER HOLEN I am, indeed.

JEFF OSBORN Hello. And I run ISC on my day job. We develop and give away open-source software for DNS and DHCP and operate the F-Root server. Next. That may be the last one. And this is the deer in the headlights moment where we stop talking fast and then stare at the audience and say, "Are there any questions?" And this is like looking at an entire herd of deer seeing headlights.

KEN RENARD No questions from over there. No, nobody's raising their hand over there.

JEFF OSBORN Hey, Dave, got a question?

DAVID LAWRENCE Hi, Jeff. Jeff encouraged me to precede the discussion. So David Lawrence, IETF liaison to the ICANN Board and RSSAC Caucus member. My question is actually for both the SSAC and the RSSAC, and the context is that the IETF currently has ongoing discussion about the use of local root resolution as an augment to the Root Server System for being able to do DNS resolution. How does the SSAC and the RSSAC see local root fitting into the DNS resolution process?

JEFF OSBORN That's an excellent question, Dave. Liman, would you like to take this?

LARS-JOHAN LIMAN I can take a stab at it. Lars-Johan Liman from Netnod, root server operator, RSSAC member. There isn't a formal decision taken or a formal standing from RSSAC on this, but it is something that can improve the local resolution for a local community using a resolver. It is something that is well-documented and well-proven to work. It is something that offloads traffic and problems from the existing

Root Server System, so there are lots of benefits with this idea. The one drawback you can find is that it's more difficult to understand the DNS patterns in the world. When we have a unified Root Server System where we can do measurements and understand how traffic is routed on the network, we can do good observations there and draw conclusions. If the entire world was to switch over to local roots everywhere, the root servers would not see that traffic, and that's a slight drawback. There can also be some drawbacks regarding fault isolation. There are pros and cons there. You have the pro, the upside is that if there's a problem with that local root service, it will only hit the community around that specific resolver. Whereas, maybe if the problem sits with a global root server, we have a lot of expertise to draw on to look at and address the problem, which might not be available to the local root operator with this resolver. So these are a few observations on that. And mostly it's something that at least I encourage people to do, or at least look into doing. It's well-documented. There is an RFC document that describes how to do this in a well-defined way. So mostly positive, I'd say. Thanks.

RAM MOHAN Are there any SSAC members who would like to speak?

JEFF OSBORN By the way, Warren is here.

RAM MOHAN Warren is here, but Warren is quiet, so he doesn't want to respond to this. That's how it goes.

JEFF OSBORN Would you like-- you're being thrown a softball, Warren.

RAM MOHAN Okay, so let's go to the next question. The lady there, please use your mic.

HOUDA CHIHI Thank you so much for the great presentation. My name is Houda Chihi. I'm ICANN Fellow 86. The question is that I heard about the possibility of opening of a program of SSAC for fellows. If you can elaborate more, please.

TARA WHALEN So is this the question about the research apprenticeship program? Yes. So if so, we're running the pilot this year. We haven't yet determined what we will be doing when we repeat it. But to sort of tell you generally, we were looking in this one for people who had a skill set where we could apply their skills in a particular work party. So the idea is if the nature of the work that's happening in one of these technical areas is something you have expertise and can produce a piece of work to contribute in a limited period of time. So a little bit like an internship would be, but on one of these subjects. So in the future, you have to look for a call, and we do try

to make it very evident for, for example, people who are in sort of NextGens and Fellows to be hearing about that. But it should be available for those folks to choose someone from. So I encourage you to keep an eye out, and also you can keep in contact with any of us at any time so that we can let you know when that's happening.

RAM MOHAN Who's got the next question?

DAN GLUCK Ram, we have a hand in Zoom.

RAM MOHAN Okay, let's go to the Zoom question.

SUNCICA ROSIC Hello. Suncica, for the record. Thank you for the overview. I have a question about delegation signer record automation, as discussed in SAC126, and specifically about the pull-based approach, where the parent side collects the DNSSEC parameters from the child DNS operator. I found the publication very interesting, and you also acknowledge the drawback of this very precisely, which is that it is not exactly known when the child zone would publish the CDS key or CDNSKEY, and therefore scanning is required. However, full zone scanning is likely to be inefficient, as it is expected that only a few DS records would result in an update. So I wanted to ask, in your

view, what would be the best practice for registries and registrars to balance the scanning efficiency cost with the security needs required for the bootstrapping? Thank you.

RAM MOHAN Thank you. Jim?

JAMES GALVIN Suncica, hello. Jim Galvin. I'm not going to be able to answer your question precisely here, but I happen to know that you're going to be in Vienna at the IETF, and the gentleman who should answer that question is Peter Thomassen, and he will be there too. So I think I will make a point of connecting the two of you, and you can have an extended discussion about this topic, and that would be very helpful. Thank you.

SUNCICA ROSIC Sounds great. Will reach out to Peter.

RAM MOHAN Maarten, let's go to you.

MAARTEN AERTSEN Yeah, just a brief follow-up to what Tara just answered with respect to the apprenticeship. I happen to know that the ICANN website allows you to set up notifications for stuff that is published, and I checked at the previous Mumbai meeting with someone who is

interested, that you can actually subscribe for email alerts specifically for this type of content change on the website. So if you don't want to ask a lot of times if it's open already, you can set up an email notification if you're interested. And I guess this also goes for the open window for applications, because that's also a content change on the website. So for anyone who's interested to hear about this type of thing, yeah, maybe have a look at how the ICANN website facilitates that.

RAM MOHAN Who's got the next question? Please.

ANDREW CAMPLING Hi. Thank you. Andrew Campling. It would seem rude not to talk about agentic AI, so I've got an agentic AI question. Current forecasts from the Contracted Parties Summit suggested that agentic AI will lead to a 4-to-15-fold increase in the number of domains registered by 2030. Do you think that will overload any parts of the DNS ecosystem? And I'm thinking particularly about things like some of the back office systems for registries and registrars, not just the obvious things like the root server, for example.

RAM MOHAN Well, we have some registrar members from the SSAC here. I can speak on behalf of at least one of the registries, and Laurin, the

work party chair, is also here. So why don't we start with the registrar, go to the registry, and then go to you, Laurin. Jonathan?

JONATHAN FRAKES Thank you very much. I'm Jonathan Frakes. I'm a member of SSAC, but I also have been a registrar for years, so I have a little bit of insight into that. I think we're delighted if there's an increase in registration, hopefully positive registration, and we're putting in the appropriate guardrails to ensure that there'll be positive registrations as opposed to abusive registrations. But if I had a crystal ball, I don't know if I would've gotten into this business. I would've probably invested in real estate or something, as far as this goes. I look forward to what agentic will do for us. We're looking at a variety of things to help curb negative activity and detect positive activity and enhance and encourage that. So sorry for the kind of word-salad non-answer, but I'm not a good futurist. Thank you.

RAM MOHAN Thanks, Jonathan. I've worked with the registry. From the registry side, I think the biggest thing that we're looking to do is to make sure that the processes for handling and for responses, and for exceptions especially, are robust. Because where we are anticipating the scaling issues are not in the regular registration and the EPP-oriented, automated-oriented things. Those have plenty of space and scale. And at least in our experience with registrars, we see most of the registrars also have a lot of scale on

that. But where we're spending quite a bit of attention on is on the perhaps side, but ancillary things like being able to provide adequate support, being able to respond to automated inquiries that come in that are driven by agents or things like that, as well as the exception handling pieces. Our anticipation is that among the biggest impacts of what's happening with agentic access to systems is the speed, as well as the scale, is where we're expecting to see the maximum amount of change. So we're making sure that our processes scale up to handle the speed and scale. Laurin?

LAURIN WEISSINGER Yeah. Thank you. I don't think I have much to add because we had two perspectives, and I largely share what has been said. The core systems are very scalable, protocol-sufficient, et cetera. The key is more in the, okay, how would certain processes, let's say, around registration management change, and are these more side systems capable to handle it? But what I'm hearing is this won't be happening immediately, and so as with everything else, things will scale accordingly.

RAM MOHAN Jeff?

JEFF OSBORN You threw in root server in your question, so I'll respond. I've never heard a forecast that literally doubles the size of the number of TLDs by 2030, so that would be a trivial task for us. So in terms of

capacity, I don't technically speak for anyone else, but I can't imagine it's a problem simply doubling the size of the zone.

LARS-JOHAN LIMAN

So Lars-Johan Liman here again. I support that, but I would also like to add that the DNS tree as a whole is very easy to expand under the root level. So if the number of domains multiplies by orders of magnitude underneath the root, that is not a problem at all because you can scale up the number of servers and the number of pointers to these servers. That's very easy. So, the only single point we have is the Root Server System, but as Jeff said, the root zone we have today is quite small in comparison to many other zones. So we know that it's quite possible to handle much larger zones in the root servers as well as at any other level in the tree. The other thing you might want to worry about is the level of queries. Of course, the shape of this DNS tree will change a little when you add more top-level domains. But we've gone through this process once without any hiccups whatsoever, so going once more is not something that keeps me up at night. And again, it will not happen overnight. It will be a gradual shift. And the Root Server System that we have is so massively over-provisioned that this is not something that should even make a dent in the statistics. Thanks.

RAM MOHAN

Any other responses to that question from the room? Okay. Who's got the next question? Maciej has a hand.

MACIEJ PIASECKI

Hello. Maciej Piasecki. I'm with EURALO, where I'm one of the training leads for the phishing campaign. And as a semi-technical person, because I'm a historian who just got into cybersecurity a few years ago, I can't help but notice there seems to be a big discrepancy and a knowledge gap between what you guys know from the technical perspective and what the other parts of the community seem to put on the table. So what would you say are the essential topics the whole ICANN community should get up to date right now to have meaningful discussions with you in six months, one year's time?

RAM MOHAN

So let me speak for the SSAC piece, and then Jeff, I'll come to you. I think on the whole, it's the five key topics I talked about: DNS abuse, DNSSEC, the impact of alternate name systems and how they interact with the DNS, new gTLD program and name collisions and other aspects of the new gTLD program that impact security and stability, and the policy and tech intersection for security, stability, research topics that have to do with Internet governance. So I think those are the five big things, and what we're hearing from members in the community is, "Why don't you have something on AI yet? Why don't you have something on blockchain yet?" And in general, our response to that is, we try to say something if we have something to say, rather than because it is the hot topic. So that tends to be our approach, and we tend to be very allergic to kind of

either repeating what's already been said elsewhere or to boiling the ocean. Jeff?

JEFF OSBORN I'm going to hand this to Ken Renard.

KEN RENARD Hi. Great question. Ken Renard from Army Research Lab, one of the root server operators. From the RSSAC perspective, the Root Server System, there's a lot of misunderstanding about the Root Server System in this community here, especially when you get out into governments, regulators, things like that. What we would strongly encourage is to find out how the Root Server System actually works. Remember, RSSAC had a very narrow scope. The Root Server System is actually a much narrower scope than people think. We don't control the contents of the root zone, and there are so many things that we don't actually do. One of the best ways to get up to speed, we do a "How It Works" session at ICANN meetings, I guess not during the summers. That's a great way, as well as there's an ICANN Learn module on ICANN's website on how the Root Server System works. And we love to talk about this stuff. We're nerds, we're engineers, so please come see us. We love to talk about it.

JEFF OSBORN Any other input from the RSSAC folks in the room? Thanks.

RUSS MUNDY There's a question in Zoom.

JEFF OSBORN And who's got a question?

DAN GLUCK We have a hand in Zoom from Charles Grant.

JEFF OSBORN All right, please.

CHARLES GRANT Hi. Yeah. So Charles Grant from Dominica in the Caribbean. My question is, SAC115 and the current DNS abuse and AI workstream focus on abuse mitigation. Caribbean ccTLDs and small island registries frequently lack the legal framework, staffing, and contractual leverage to suspend abusive domains at the speed of the SSAC recommendations. Is the community developing a tiered or proportional DNS abuse response maturity model specifically for micro-registries, rather than applying standards designed for larger TLDs and 100-person abuse desks, so basically smaller registries? Thank you.

RAM MOHAN Thank you, Charles. That's a great question. So I have a very personal point of view on that. If you take the standards for

response to DNS abuse, and if you perhaps dilute them or if you make them proportionate, if you will, for a micro-registry, that's exactly where all the abuse will flow to, because the guys who are watching are going to look for where the weakest points are. So my thought there is perhaps there is a lot of work that has to be done in both the development of capacity in small islands, where it doesn't exist, number one. And number two, maybe in those areas, maybe the approach could be more regional in nature rather than national in nature. But it's a really important problem, and it's a pervasive one. And in my experience, I think that's part of the reason why in many of the micro-registries or the much smaller TLDs, you find bad actors preying on them. And it's not for lack of good intent, but it's often because of lack of good resources. So I agree with you, it's a serious problem, but I would strongly push back against the dilution of any of the standards for appropriate and swift mitigation of DNS abuse, to reduce that in some way to handle a micro-registry or a small island nation. Open for other perspectives or other thoughts from other SSAC members. Rod, anything you want to add?

ROD RASMUSSEN

Thanks. Rod Rasmussen, SSAC member. Yeah, I agree with you, Ram, on this, where abuse will flow. I would take the argument that if you are provisioned to provide a large number of registrations, you should be provisioned to handle a large amount of abuse on

those registrations. If you're not provisioned very large anyways, you probably won't see a lot of abuse, so it would scale that way.

RAM MOHAN Thank you. I see a hand raised there.

NIGEL CASIMIR Thank you very much. I'm Nigel Casimir from the Caribbean Telecommunications Union, one of the observer members on the GAC. I'm very happy to hear you say, developing the capacity in the small operators or small markets as a part of the solution for this question raised by Charles. And in fact, I think there'll be a lot of discussion on that in the session after this one as well. So it's a particular issue that we from, I'm from the Caribbean region, as a regional organization, that we've been trying to push, and this is why we often have representation at ICANN meetings, to represent the interests of these small voices that are not often heard. So I'm happy to hear you say that, and I'm sure we'll explore it a lot more in the next session. Actually, one other thing I would like to say is that one of the things we had to do, for example, in our region, there is ARIN, for example, which is accustomed to dealing with larger operators. And we had to advocate for ARIN to put in special procedures, establish policies and special procedures for the small markets in the Caribbean, which was done a couple of decades ago. So I think making space for those voices is something that needs to happen. Thank you.

RAM MOHAN Thank you. What about from the root server side, for a question like this?

JEFF OSBORN I think, okay. It's important to remember, I think like Liman said before, the topology of the DNS tree is such that the root system really doesn't get affected by it. If you think of us as a directory of country code numbers, the fact that complicated things are going on in the 193 countries just doesn't affect us. We really have a very small remit because we really have a very small amount of information to deal with.

RAM MOHAN Fair enough. Thank you, and just a quick rejoinder to what you were saying. The SSAC is quite interested and is willing and able to provide assistance in those capacity-building efforts. We have not only technical experts in this area, but we also have developed over the years a great deal of content that might be able to be repurposed into training and other capacity-building things. So please do engage with us, and you can engage with the SSAC staff to help that coordination happen. Thank you. Liman.

LARS-JOHAN LIMAN Thank you. Lars-Johan Liman here again. I would like to add one thing, though, that when I interact, which is very seldom, but there is a relationship with the content of the root zone and the various

registries for top-level domains. As a root server operator, a top-level domain is a top-level domain, and there is no difference between them. So whether it's a problem with the .com zone or with Dominica, it's the same approach from my side if I have to do something, again, which is very seldom, because the problem usually sits elsewhere, as Jeff said. But the resources from Netnod, when it comes to providing support in problematic cases, are the same for any given TLD. Thank you.

RAM MOHAN Who's got the next question? Please.

JEFF OSBORN If nobody gets one, one I get asked a lot after these sessions, I figure I might as well make it public. That would be the question of: how do I get a root server? There are a bunch of us up here. There are thousands of root server instances out in the world, and I think six of the root servers are represented in the room right now. A number of us will provide a root server instance to anybody who wants it. The easy way is to tell us where you have-- we specify, for instance, a particular model of a Dell computer in a rack with three network connections and a power plug. We very generally will buy the equipment for you if that's a hard thing. We're really just insisting, if you're interested in having an instance, you should have access to a location that's suitable, three links in, and power. And it's seriously that simple. The last time we did one of these, we had several up in a matter of weeks. And if you wanted that, I just

Googled, "Can I get an F-Root server?" And it came up with the application. The form is really simple. It's about a page and a half long. The process is simple. And the technology required is just not much. If you're interested in doing it, you know enough to do it. So we would encourage it. We add them when they're needed, as often as anybody is interested in it. Anybody else want to have a comment on that or just leave it as the commercial portion?

LARS-JOHAN LIMAN

Lars-Johan Liman here from Netnod. We have a similar approach. We have a similar form. We try to interact with the entity that is looking to deploy a root name server, but we are a bit restrictive in how many and where we can deploy them because it uses up resources at Netnod, and we don't have infinite resources. So it's a bit of a negotiation to find the right place where we have the most effect for deploying a root name server, and again, where we can find the financial and also technical stability. It's very important that a root server can receive local staff that can support it. And we need to feel secure that the future of the root server is also, how should I say, is well cared for into the future. And that has been a problem that we've learned from. Thanks.

RAM MOHAN

Let me bring up a--

TARA WHALEN

There's a question. John Levine had a question.

RAM MOHAN Ah, John, let me go to you.

TARA WHALEN Do you have a mic?

RAM MOHAN John Levine?

JOHN LEVINE Me over here, yeah. I was offering to respond to the question about the delays involved in the scanning for DNSSEC updates. But actually, I had a private chat with the woman who asked about it, and the answer is look at RFC 9859, which Peter and I published, which basically is a way for the operator of the updated zone to poke the parent and say, "Hey, scan me." So that gets you a reasonably quick scan without adding new security issues because the scan still has to satisfy everything it would have otherwise. And I sent her some notes, but if you look at that RFC, it should be pretty straightforward, and we designed it in a way that should handle both registry and registrar scans, depending on your local policy.

RAM MOHAN Thanks, John. Let me just pivot to another question that the SSAC is often asked, and that is: I'm really interested in the work that you're doing. We're glad to see that you're open by default. We come to the meetings. We see the work parties. Really interesting

work. I have something to say. I have something to contribute. How do I get engaged? How do I become a member? And what does that take? So that's something that we get. And is there a deadline? Is there a date by which I have to apply? What is the process for my application to be reviewed and evaluated? So that's a question that we're often asked. And Tara, you are the resident master of that piece, so why don't you take this?

TARA WHALEN

Yeah. If I want to start with the deadline first, it's the 30th of June, so the end of the month. If you've been thinking about applying, you should keep that date in mind, so that you're ready to get your application in. So how to get here, I think Ram set it up pretty well. The first thing you need to do, I guess, is to have a good sense of the nature of the work. So for those who have already been attending the meetings, looking at our presentations, reviewing our documents, that is an absolute bare requirement because obviously you need to know this is the sort of work that you're interested in and could contribute to. And what we're really looking for is people who can contribute and deepen and extend that type of work. So because we do a lot of the work through the advisories, if you have a look at one of those and you're trying to say, "Am I ready to apply?" Put yourself in the position of someone who would have created that document and think about, first of all, you should understand the majority of it. And we have a lot of topics. You don't necessarily have to be 100% on 100% of them, but a substantial number so that you can contribute to, for example,

more than one subject. And think about what section you might have written, or what section you might have deepened, or what section might be missing from the document that you could have put in that would have made it better. So how does your piece make our work better and stronger in some way?

And people come to us from many different paths. We have people who have operational experience or research experience, or they work at registries or registrars or network operators or universities, and they all have skill sets that are sort of deep and broad in a technical sense that we need to help us do our work. So the calibration can be hard. Think about that for a while. Sometimes you may be ready earlier than you think. Then you come into the assessment, which can also be difficult, but we have a very thoughtful team of people who look at the applications. We also have to look at what we're missing in SSAC at the moment. So we sort of want complementary things sometimes. So not just everyone with the identical skill set, but again, some extra pieces so that we're not completely redundant. So sometimes you could be very mature in your career with lots of skills, but there are already four other people doing the same thing, which means that it may not be the right time for you, even though you're qualified, because of the composition of the particular group.

So if you submit an application, there's a sort of "how to get involved with SSAC" on the SSAC page on the ICANN site. Then there will be a process there where you will talk about your background, give us information about you and your interests, and

why you want to be involved. And then our committee will look over those things and select among the candidates we think are likely to be the best match and do interviews with them. You sort of sit collectively. As many things, I know ICANN, we all move so quickly to get things out. It takes us a while to do it. So we appreciate your patience while we go through this. But generally, we'll get everyone in place by the end of the year for this. And we are also very friendly. We hope that people come and talk to us. I will also note people who give presentations about things, for example, like the NextGen, we love seeing the kinds of things you contribute and hearing about the ways in which you present your work, what you're doing in other communities, and that is great evidence for us. That's a great way to connect, and we're very friendly. Talk to us at any time with your questions, knowing more about SSAC, and we're very happy to help you out and put you in a good position.

RAM MOHAN Jeff, how does someone join the RSSAC Caucus?

KEN RENARD All right. This is Ken. So the RSSAC Caucus is similar. It accepts applications. We accept applications on a rolling basis. You can find the Caucus webpage pretty easily by searching on icann.org. Typically, we like to see some expertise in DNS and authoritative server experience, and experience with the root-type-level parts of the DNS. And you can submit an application, and we usually

respond in about a month. And you're welcome. Usually, after an ICANN meeting, we get a couple new applications, and we like to hear from people all around the world, people with different backgrounds, and we appreciate your help.

RAM MOHAN Thank you, Ken. Dan?

DAN GLUCK Yes, we have a hand from Enoch Singano.

RAM MOHAN Enoch, we cannot hear you, so perhaps check your mic.

JEFF OSBORN The mute isn't in Zoom. It's farther back on your side, but we can't hear you.

RAM MOHAN Would you like us to read out the question that you have written in the chat? Okay, wonderful. So, Enoch Singano from the Malawi Youth IGF. The two questions, the first is, as the Internet ecosystem prepares for future cryptographic transitions, what DNS security areas should technical practitioners be focusing on today? So that's the first question. Would anyone from SSAC or the RSSAC like to respond to that? Jim?

JAMES GALVIN

So I'll add some personal thoughts and offer two suggestions, and maybe this bleeds into the second question, too. I think that as the future of technology advances, and in particular, quantum cryptography and quantum computing comes to bear on us, I think being able to do algorithm rollovers and to do them effectively and consistently as part of your ordinary key signature rollovers is important. I don't think we've exercised that as much as we probably should, and experiment with that, and make sure that we have full control over that. The second issue that I would offer from a DNSSEC point of view is greater automation. I think that one of the most significant problems that we have when we see failures is about configuration errors. That's something which happens a lot, and also, key changes and key rollovers and miscommunications, miscues that happen. So being able to support greater automation in the management of keys, DS automation in particular, and SSAC has focused on this and has a report that it has put out about this issue. We had a question earlier, a detailed question about this topic. I think that these are two very important areas from a practical matter for the ecosystem at large to pay attention to. Thanks.

RAM MOHAN

And to add to that from the SSAC, our SSAC member, Peter Thomassen, he says cryptography in the DNS is involved in three broad areas: DNSSEC, encrypted transport, and potentially certain

record types that convey cryptographic information, SSHFP, TLSA, et cetera. Now, for the first DNSSEC, practitioners do not need to worry now because first engineering has to happen, so it's a later concern. For the second encrypted transport, well, that's going to get migrated with the usual TLS stack migrations. And third, for record types that convey cryptographic information, what Peter says is folks need to look at their inventory of cryptographic applications, including, but not limited to ones reflected in such DNS records, and migrate them. So those are the security areas that Peter suggests you should look at. Liman.

LARS-JOHAN LIMAN Thanks. Liman from Netnod again. Thank you for all that. I totally agree with both of you. I would like to add one more thing, which is that for the community that deals with DNS operations to learn and find out where the discussions about the future happen, so that they can follow these and be on top of changes and be very quick in adapting when things happen. So familiarize yourselves with where are these things being discussed, in the IETF, in DNS OARC, possibly here in SSAC and the DNSSEC workshops and whatnot, so that it doesn't come as a surprise, that you're not surprised by having to make changes suddenly, so that you've been following what's going on and can be prepared. Thank you.

RAM MOHAN Thanks. And there was a second question also from Enoch Singano from the Malawi Youth IGF. And that second question was, what

DNSSEC deployment challenge concerns SSAC members the most over the next few years? So Jim, you said you wanted to cover that. So do you want to take that first, and then I'll read out Peter's answer?

JAMES GALVIN Yeah. I think I actually did try to answer that a little bit when I talked about the DS automation and the SAC126 discussion that we had before. I think that being able to manage your keys and your key rollovers in an independent way and not have to do it manually is an important consideration. And you're limited from service providers in order to do that. There's a coupling that's missing between registrars and DNS service providers. That's the DS automation issue. And so that's an important thing that has to be captured and addressed and moved forward with. And there's work to be done on the ICANN side in that space, too. Thanks.

RAM MOHAN Thanks, Jim. And SSAC member Peter Thomassen responds to the question of what DNSSEC deployment challenge concerns SSAC members the most over the next few years. His response is, number one, automation in general, and number two, getting automation in early enough so that post-quantum cryptography migration can happen largely automatically. Warren, over to you.

WARREN KUMARI All the way in the back. Yeah, my biggest concerns are the fragility right at the moment. Sometimes it bites people badly, and then they don't want to do it again. And also explaining the utility of it to people. Currently, it doesn't seem as though people are clamoring for it because the cost-benefit analysis isn't really clear to them.

RAM MOHAN Thank you, Warren. Other questions? We're coming up to about five minutes left, so bring your questions quickly. Please.

ANDREW CAMPLING If no one else is biting, I will. Since you touched on this topic, with sort of post-quantum cryptography, how ready do you think the systems are? Current forecasts say by 2029, there'll be commercial quantum computers available, according to some companies, which to me suggests some state actors will have them in advance of three years' time. Is the DNS ready for that?

JAMES GALVIN So I'll start and answer, and I'm sure we'll get some feedback from Peter, who's out there listening to us, and offer some more. But I think it's important to separate that into two problems. From the cryptography side, DNS is ready for that. It already has built in the ability to change algorithms, and to that extent, the system doesn't care about that. You just need an algorithm rollover and new keys, and then all of that works. On the other hand, that does mean that resolvers who are going to take advantage of that cryptography,

there's deployment on that side that has to happen. So the DNS system from an authoritative service point of view would be prepared to handle this. But on the validation side, you really do have a significant deployment issue that has to be captured, that would have to be addressed and would have to be dealt with. The cryptography is a separate problem that doesn't really happen here, doesn't really happen in the IETF. There are other bodies that do the cryptographic analysis that establish algorithms and their purposes, their characteristics, and their roles and how they work. I think that we're ready to accept a proposal for a new algorithm, and then we have our own set of deployment issues to deal with that. So two different problems. Hope that partially answers your question.

RAM MOHAN Thank you. Liman.

LARS-JOHAN LIMAN Thanks. Liman from Netnod again. In this context, the good news for root server operators and operators for authoritative DNS services is that we don't have to bother, more or less, because the signing of the data typically happens as a transaction with the DNS data before it's put in the server to be served to the Internet. So what the authoritative server, where the root server is, is just one part of that entire system. The authoritative servers have prepackaged, already crypto-treated material that is just handed out on request. So for the authoritative side, there isn't much of a

change at all. As mentioned, on the resolver side, it's different because you have to update the software so that it can use and take advantage of the new crypto algorithms that are being evolved and deployed and put into code. And it's a little harder to interact with the resolver community. The authoritative server operators, you can find using the DNS. You can see where the pointer's going and say, "Aha, here's a server. Someone is operating a server here. I can probably reach out to that person if needed." With the resolver operators, it's much harder. It could be someone's house. Mine, for instance. It could be an office somewhere. You have no clue who these are, so it's very difficult to reach out to them and have a dialogue with them and say, "Please follow what's going on. Please be prepared to update." But it's doable, and we see more and more automated software updates, and that's very good news for the software community in general, and the DNS system is part of that. Thanks.

RAM MOHAN Thank you. Warren?

WARREN KUMARI Yeah. Warren Kumari, SSAC. I think my views aren't quite as rosy as Jim's, and maybe not Liman's as well. For the Root Server System, yes, it's largely, "Here is a blob. You serve it as always." But for other authoritative server operators, they're often the signers as well, and they're going to have to do some work. But apart from that, almost all of the post-quantum signatures are substantially larger

than traditional signatures, and in almost all cases, they won't fit in a UDP packet, which means many connections would drop to TCP, which potentially has implications. There is also, for the few root server operators who are doing DNS over TLS or DOE or any of those sorts of things, they potentially have implications as well. At the moment, that's a small number, but it's not purely-- largely, though, what you said. The root serves a blob, and it's largely exempt from this issue. But I think the rest of the DNS ecosystem potentially does have a fair bit of work.

RAM MOHAN Thank you, Warren. SSAC member Peter Thomassen has this response for the question on how ready do we think the DNS systems are ready to handle PQC. He says applications using encrypted transport will be ready, TLS. Most other IETF working groups, such as SSH, et cetera, also are making good progress. DNSSEC may not have a nice answer other than that allows staying on UDP. His stake is that if that happens, it'll likely to just move to TCP, as Warren was just saying, more broadly, and deploy algorithms that don't fit in UDP. But Peter also says there are experimental implementations and benchmarks that are available. And for more detail, attend the post-quantum DNSSEC side meeting at IETF in Vienna that's coming right up. And the other thing that he's adding is that storage encryption is usually symmetric and therefore not as affected. Other questions? Last

question. Well, if there are no last questions, we'll go to last comments. Jeff?

JEFF OSBORN

Thank you all very much. I think it's always instructive and interesting, but I'm never shocked by the questions, so that's probably a good thing for now. I think AI will continue to be an investigative concern. It's definitely too early to panic, but if nothing else, it makes excellent cocktail party conversation. So thanks. It's always been fun. We appreciate SSAC giving us this opportunity. And back to you, Ram.

RAM MOHAN

Thank you. Tara?

TARA WHALEN

No, just thanking everyone for being here. We're here. We love getting feedback from the community. We like connecting with you all, and so I appreciate your attention. I'm also going to point out, I think this is a joint meeting with the RSSAC, the SSAC, and the HVAC. So you've had to contend with all this system today, so I appreciate you dealing with those audio challenges.

RAM MOHAN

And that concludes our session. Even though the recording is going to end, let me also ask, I know there's a number of NextGeners in here and Fellows, and I had asked you to come to this meeting.

Please come up to the front here. I think I saw Barry get up at one point, and I think he might have left the room. But please come up, NextGeners, and let me do what I said that I would do and make some introductions. Recording stopped. If SSAC members would like to meet them, please come up so that we can connect people and put you together. Thank you.

[END OF TRANSCRIPTION]