ICANN84 | AGM – Joint Session: ALAC and SSAC
Sunday, October 26, 2025 – 13:15 to 14:30 IST

MICHELLE DESMYTER: Hello and welcome everyone to the joint session, ALAC and SSAC. My name is Michelle DeSmyter and I am the remote participation manager for this session.

Please note that this session today is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, French, and Spanish. If you would like to speak during this session, please raise your hand in Zoom.

When called upon, virtual participants will be given permission to unmute in Zoom. On-site participants will use a physical microphone to speak. Please state your name for the record, the language you will speak, if speaking a language other than English, and please speak at a reasonable pace. I will now hand the floor over to Jonathan Zuck, ALAC Chair, and Ram Mohan, SSAC Chair.

JONATHAN ZUCK: Thanks, Michelle, and thanks again for members of the SSAC for joining us. We've been forming a tight bond and we learned this morning that the NCSG is jealous of our bond. So, they want to form a relationship like that with us as well. That's very exciting.

We have a lot of complimentary interests between us, and finding those synergies and finding how to help each other, I think, is our goal.

We probably need to be doing more intersessional discussions to get more progress and more momentum, but we're always excited to hear the new things that you're working on and what, if anything, we can do to help evangelize them, whether it's within the ICANN community or out into the broader end user community. We're excited about some of the stuff we've got on the agenda. Once again, welcome.

RAM MOHAN

Jonathan, thank you. This is the original partnership, so it doesn't get displaced or replaced. That's just where it is. We're very pleased to be here. We've been really encouraged by your continued welcome to the SSAC, to our community, and the tighter integration that we've been working on. We have at least one worked example of how this could work well, and there's more to come.

Really, I think today we have some parts of today's session where we have some presentations, but we have other parts that are about a conversation amongst us and to see what we can do to really improve the ecosystem, to kind of elevate both the education and understanding, but also the security ecosystem that is out there. Those are our shared goals. Happy to be here.

Today, we wanted to spend quite a bit of our time chatting a little bit about a report that we have just published, SAC132, which is a report on the free and Open-Source software and its indelible nature, especially in the critical infrastructure pieces that we are involved in. We have one of the co-chairs of that Work Party, Maarten, right here to my left, to be able to speak to that.

Then I want to chat a little bit and give you a sense of what are the other things that the SSAC is looking at and what are the things that we're working on and to, again, both to inform but also to consult with you on and see if you have any inputs into what we're doing.

A couple of the pieces that we're working on are in early stages, in chartering stages, so this is the best opportunity to kind of shape and influence where it might go. We'll take it from there. I think Suzanne is here as well from the SSAC's point of view. She is one of our representatives to the Review of Reviews. She's right there in the back. I look forward to that conversation. I know that one of the co-chairs of that comes from the ALAC. Avri is here, so look forward to that conversation should we get time to get to that. With that, let me hand it over to you, Maarten. Please.

JONATHAN ZUCK I just want to say that at this meeting more than any other, it seems we've been having trouble hearing each other. I don't know if the levels on the microphones are different or it's the room or whatever it is, so however close you think you are to the microphone, get closer. Just get to know it really well. Become intimate with the

microphone because we end up stopping almost every speaker and asking them to get closer to the microphone. So, I thought I'd try to tell you up front.

RAM MOHAN

Thanks. Sounds good. Of course, there are these headsets that you could use if you want to enhance the effect. Maarten.

MAARTEN AERTSEN

Thank you, Ram. Thank you, Jonathan. Thank you to the ALAC for the opportunity to speak to this latest report. My name is Maarten Aertsen and I'm the co-chair for this piece of research that we did. Next slide, please.

SSAC usually writes rather technical reports. One slide back, please. This is not one of them. So, the ICANN Board is not the primary audience for this document. It's the Internet community, and in particular, beyond the Internet community, policymakers and regulators around the world. And that's why we need you because for this document to actually make a difference out there, it needs to reach people locally who are talking to policymakers in their respective country.

So, that's a little something up front because I know that in this meeting we like topics where we can collaborate. So, we did some research, but research on its own doesn't move anything, right? So, let's talk about software. And specifically, the reason why we talk about software today is because software is increasingly being

regulated around the world. Sometimes the production of software is being regulated. Sometimes its use in critical infrastructure is being regulated.

So, what we thought we would do is figure out what is the software that is used in the domain name system that we care so much about. Next slide, please. And what we found, if you want to summarize this report in a single sentence, is that the DNS is built and sustained on Open-Source software. And this is not advocacy. This is not saying that that's a good thing or that it's better somehow. It's just a statement of fact of how this infrastructure, globally, is actually built today. Next slide, please.

So, Open Source software, what is that anyway? So, it's about a license on software that allows for freedoms. So, this is not about things without a price. It's about freedoms. And these freedoms are to use software for any purpose, to study it, including usually the source code, to share it with whomever you like, and if you change anything, you can still share it. So, these are the freedoms that collectively create a fundamental different ecosystem for software development, for distribution, but also for maintenance, as compared to the opposite, which is proprietary software.

So, there are some philosophical differences about how to name this. For this report, we choose free and Open Source software because it's kind of the way to keep everyone happy. But maybe some of you know this phenomenon better as just Open Source, and that's fine, too. Next slide, please.

So, why is it relevant what type of software people are using? Well, if you start regulating the space of software or its use in critical infrastructure, you might take a view that is a bit more traditional, where you look at supply chains and you think, well, if we just introduce some requirements at the start of this chain, it will just trickle down to whoever makes this, and then we have a policy lever, right? You can do contractual obligations and work from there.

So, in free and Open Source software, there is often no contractual obligation or relation between the developer of the software and the user of the software. So, a volunteer can write code that a top-level domain operator ends up using without any payment, for example, without any relationship or without any ongoing obligation. And so, this is just an example, but this is why supply chain thinking fails for FOSS.

You can't, for example, impose contractual obligations when there is no chain of contracts. It's hard to hold someone liable when they're not actually your vendor, right? So, this is a different model that applies to this ecosystem of software.

Now let's look at the frequency of this. So, we had this bold claim, right, that it's everywhere, and we'll now quickly go through some of the data in the report. Next slide, please. So, if you look at the root server system, we looked at the information published by the root server operators about the software they use, and you see here that at least 9 out of 12 exclusively use FOSS.

If you look at the remainder, they sometimes use a proprietary software, but then have FOSS as a backup or for diversity. So, this number is even larger if you make the claim a little bit less conservative like we did here. So, this is not a small percentage, right? Next slide, please. Great.

So, if you look one level down at top-level domains, perhaps for your country, and you look at the infrastructure providers that provide services to individual countries, to gTLDs, we find that 9 out of 10 biggest ones by number of TLDs uses FOSS to do hosting. If you just look at countries, and for now not look at the gTLDs, it's 20 out of 25, and if you do not look at IDNs for one second, it's 23 out of 25.

So again, these are not small numbers, and all these entities are completely free to do whatever they want, right? So, there's no one saying they should, it's just in practice it turns out that this is the software they choose to provide stable infrastructure. So, some examples here, Nominet for .UK uses FOSS name server software, .CN for China is using FOSS name server software, and I can go on. Next slide, please.

JONATHAN ZUCK Just a quick question, the fact that there are some using commercial or proprietary software, does that mean that there are equivalent products to these Open Source products, or is there some other type of difference in terms of capabilities or something

like that that's driving the minority here to use something else? Why wouldn't all of them use these tools?

MAARTEN AERTSEN: So, there's definitely also proprietary implementations, yes.

JONATHAN ZUCK: There must be, right? Because there's some grey boxes, right?

MAARTEN AERTSEN: Yes, exactly. But depending on specifically the type of software, this software is then for sale or not for sale. So, there are some operators of critical infrastructure who have the excellence in-house to build a proprietary alternative, which is then their own, and they're not selling it. There're also some operators on the market who are selling proprietary name server software, but if you look at the popularity, it seems that the FOSS variant is rather popular at the moment.

So continuing, if we look at another slice of data that we gathered, next slide, please. So, in Registry Systems, so the registry being the database where the domains are listed for then to be published in a DNS later, right? So, there's two models here. So, there is the model which is entirely FOSS, where the registry is FOSS from beginning to end, and examples include FRED by the Czech Republic's ccTLD. It's being used by 12 country code TLDs, so this

shows that FOSS is viable here. But then the second model, which is actually what the majority of big registries use, it's proprietary.

However, if you ask them about it, it turns out that the software they have built themselves, and these are proprietary systems that are not built from scratch, they build on top of a foundation that is provided by FOSS. So, sometimes it's customizing components, sometimes it's integrating components, etcetera, etcetera.

And some examples, like all major registries we surveyed rely on some FOSS components, like a database, a web server, application server, software libraries, etcetera, etcetera. So, I'll spare you the details, but here again we see a lot of FOSS. Next slide, please.

Resolvers, like the query side of the DNS, right? So, here it's very hard to do measurements, and so we couldn't. But what we do know is that there is a substantial presence across the entire resolver ecosystem. So, 80% of users worldwide we know to use local resolvers, and these are predominantly FOSS. There is a commercial market for local resolvers, but if we have looked at the products that are for sale, and then it turns out that mostly the core of these products is, again, FOSS inside. So, that's what leads us to the conclusion that it's predominantly FOSS.

So, if you look at the cloud platforms, hyperscalers, CDNs, etcetera, there is proprietary out there, but at least four of the major hyperscalers rely on FOSS. And finally, if you look at public resolvers, there is a couple that are FOSS entirely, and CloudFlare,

we have a little case study in our report, says it's proprietary in the core, but it's surrounded by FOSS.

Okay, let's continue. Next slide, please. So, in summary, FOSS is the foundation of critical DNS infrastructure. So, in the most critical parts of this infrastructure, FOSS is the norm, and proprietary is the exception. And that's, I think, a rigorous finding of our research, and one we have not found documented elsewhere. So, this software is collaboratively developed, sometimes by volunteers, but in the DNS, usually by small organizations, and it's freely distributed. Next slide, please.

Now, why go through this effort? Well, it turns out that traditional regulation does not always fit. So, if you follow this supply chain thinking, and we've had a little slide about this earlier, right, you would locate a responsible party, maybe an operator of critical infrastructure, you would set security standards, you would hold them liable for failures, etcetera, etcetera, and then the thinking would be that this trickles down to the developer. Well, and that doesn't work here. So, sometimes there's no supplier, etcetera.

Now, what would be a wrong conclusion here would be to think that there's no contracts at all, right? So, the thing with Open Source software is that if you use this software, if you download it, there is no support included. So, if you want support, you'll have to get it separately. Now, finally, enforcement doesn't work.

Now, if you would continue doing this supply chain thinking, and you would make a local law saying, well, we want to improve

cybersecurity in our country or in our region, and so software should be secure, and these people are responsible for it, what could happen is that the projects that everyone use are suddenly exposed to a legal risk that they cannot afford to run, and they might just stop. Or they might switch to proprietary licenses, and then all the organizations around the world that end up using this software suddenly have a lot of strings attached, right? So, the software everyone depends on becomes less available and perhaps less secure.

So, what's at stake? Next slide, please. So, risk one, infrastructure instability. There is a component of innovation here. There is also the digital autonomy angle, because everyone can use this software, no matter who controls, like, there's basically no limitation of use, right? But if we get this right, we can continue the strong and sustainable ecosystem that we have today. So, in this presentation today, we are not talking about the security properties, risks of this software.

If you are interested, we'll have a longer presentation on Tuesday where we dive into more of the report, and we will talk about the properties of this software and how it's different. If we get this right, we'll have some advantages here, right? Then I'll go to the next slide, which is the end slide, and it's also the call of action to you.

So, we made actionable guidelines for policymakers in this report. There're also case studies of places in the world where they got this

right, and why we feel, from a technological perspective, how they achieved that. And the question to you is, how can we make this knowledge about what makes the Internet tick to the places where, in the next decade, people develop policy to secure their society on the digital level without mistakenly throwing out the baby with the bath water? That's it for today. I welcome you to the session on Tuesday, and I'm open for questions, should you have them.

AFTAB SIDDIQUI: Hi, Aftab Siddiqui. One question I have is, have you considered talking to ICANN Domain Metrica team, adding that force detail into their domain measurement, at least for the TLDs?

MAARTEN AERTSEN: So the question is whether we should somehow make this a property of a measurement system, the Domain Metrica, right? So, what was quite hard in the research that we conducted is that you cannot measure this from afar.

So, most of the methodology of this research is actually a survey and talking to people, and less like Internet skill measurement, because there are some features, like technical features, which you could use, but every operator turns them off because it's maybe not the greatest idea to give attackers the knowledge about what you're using.

So, we talked to a lot of people and we're really glad that we got the information from the operator community to enable us to write

this report, but that makes it kind of hard to add it to an existing metric system. We did this point in time study, and maybe we should do it again in the future, but that's it for now, I suppose. Thank you for the question.

AFTAB SIDDIQUI

Thank you for that. I just want to add, I understand that that switch is always off, so nobody gives you that information. The point is, at least, I mean, it doesn't have to be which version of bind you are using, but a Boolean value, yes or no, which suggests that whether, because the thing, if we go back to the community and say, okay, fine, force is important, and they might want to ask, okay, what my ccTLD is using? Can you confirm?

And what TLD, the top TLD in XYZ economy is this? What are they using? Then how are we going to answer that to them? So, yes, that's perfectly fine. There's a generic value of 9 out of 12, and whatever the number was for the TLDs, but then if the underlying question from the policymaker comes in, that what is happening in my economy or my country, then how are we going to respond to that one?

MAARTEN AERTSEN

Yeah, I think you make a very good point. So, we have written a report based on the data that is available to us. What we could not do is talk to every single ccTLD operator in the world. And I think that the smaller the operator, the more likely it is that they use

FOSS. So, I think a good default for conversations would be to assume that they do and have that conversation once a policymaking or regulatory initiative in your country starts and just find out.

Talk to the operator and ask if a law such as this would be enacted, would you have a problem considering what you are using? And I guess that drives a conversation about how things actually work and we had some of these conversations in the place where I live. I live in Europe, and Europe has software regulation. And there were some conversations in this area which inspired me to bring this work to the SSAC.

LUTZ DONNERHACKE

Lutz Donnerhacke for the record. Do you have some data about diversity in the core functions of the software? So, my problem is that sometimes errors happen in software and some conditions may arise and affect a lot of instances, a lot of software at the same time. So, it's good to have diversity in the software, but not diversity by name, diversity by code.

And do you have some information about if the products are really independent, developed for the code or if they share the same, develop on the same code and important points and is there some initiative to help FOSS projects which run out of resources but provide a different implementation for the same problem space so that we do not run in a monopoly for a special function? Thanks.

MAARTEN AERTSEN

So, this question fits really well with coming on Tuesday, because we will discuss some of the positive properties of FOSS, some of the specifics about DNS and some of the risks. And one of the positive properties that we describe about the current landscape in DNS is that there are these four independent organizations making primary name server software, recursive resolvers and there are quite a lot of operators who choose to run multiple alongside each other.

Now, your question is, is that diversity in name only or is it diversity in code? So, I'll put down my SSAC hat for a minute. My day job is at Nelnet Labs, which is one of the non-profits that creates this software. And I know my development colleagues have this it's almost like an honor code to not look at the source code of the other implementations, because they really, really, really want to implement the spec, not copy the behavior of the other.

Now, is this actual data? No, it's not actual data. But I think the reason why operators use diverse implementations is because they've learned in the past that having to patch one type while having the other one available is quite beneficial if you want to sleep at night. So, there's that. That's not hard data. I hope it answers your question. And I hope you'll be with us on Tuesday, because there's more to discuss about security, etcetera.

JONATHAN ZUCK

Thanks a lot. I'm going to run through the queue here. Let's in this room try to keep this on the level of the impact end users or what the kind of communication is that we might want to have around this. That's a pretty deep question in terms of from the At-Large perspective, and so that's my better use for the session, the SSAC session. Satish is next.

SATISH BABU

Thanks very much. Satish for the record. So, first of all, I'd like to commend the SSAC for this report. It is indeed path-breaking. We've all suspected that FOSS is a very important piece of the software, but we've not seen it documented, especially in these names and numbers that you are quoting here. So, I think this is an extremely important positive step forward to acknowledge the role of FOSS.

In the last session here, we were discussing several things connected, Mathias and I. We were discussing about BIND. Now, BIND is now 20-plus years old. Sorry, 40-plus years old. It started out in the 1980s in Berkeley. So, one of the logical questions that comes up is, if you have such long-term kind of software, now it is BIND 9, and there is no single entity coordinating the development of the software, in the domain of software, 40 years is really long.

So, how do you see the future? What is the evolution? What is the process that guarantees the integrity of the software? This is not my question. I'm just reflecting the questions that came up. Personally, I've been a user of FOSS from 2000 onwards, so I don't

want to be convinced about this, but this is a general question that comes up. Thank you.

MAARTEN AERTSEN: Thank you for the compliment, Satish. So, in respect to your question about BIND, I do not want to speak for my colleagues at ISC, but I think it's due to their work for 30 years, that BIND is what it is today. And that is hard work by dedicated people who also have a mortgage. And so, yes, funding is an issue for these organizations.

It's also an issue for other pieces of software which do not have a dedicated maintenance organization like ISC, where it's maybe one or two volunteers. An example from the DNS and you can find in the report is this DNS mask which has been maintained for decades by a single individual in England.

So yeah, there are unique risks to this, but there's also unique strengths and there is a balance there somewhere. And I'm sorry, I'm kind of ignoring you, Jonathan, on the end-user communication perspective. I found it an interesting question nonetheless.

JONATHAN ZUCK: Yeah, it's very interesting. I'm just trying to read the entire room and in terms of our collaboration, I'd be interested in boiling this down to what you see the problem in terms of government regulation is, because even that was somewhat abstract in terms of

supply side, who to regulate, what types of regulations are you talking about.

What affirmatively do you think that we can do through communicating about this and educating people to what's the change that we'd be trying to affect. But I don't mean to jump the queue, I apologize for that, but I just want to keep this conversation at this sort of room level if possible. Christopher Wilkinson, I guess is online. Christopher, you're muted.

CHRISTOPHER WILKINSON Oh yes, okay, sorry. Christopher Wilkinson for the record. Thank you for the presentation. I'm sure that we will be told where we can get the full report and I'll join you on Tuesday. But to pick up on Jonathan's end-user interest, how do you ensure the interoperability of the whole chain of actors in the DNS right down to the final user's computer or other application, when you do in fact submit and in fact encourage that it's possible for individual operators to improve and add on to their FOSS?

And this leads me to a more technical aspect of the question. To what extent is the FOSS software that you're speaking of in the form of IETF requests for comments, RFCs, because those are supposed to be stable. And I'm at a loss to understand how you reconcile stable RFCs, which have their own advantages in terms of interoperability, with the dynamics of different applications and different operators. In effect, especially those who add private software functions, different operators who are amending the

software which is in the basic RFC. I wonder if you could speak to that.

MAARTEN AERTSEN

I really appreciate that there's questions that we hope to answer on Tuesday, but I'll give a preview. Interoperability in the DNS space is something that is important for both proprietary and Open Source software. And I think all the developers of both proprietary and FOSS implementations work together in places like the IETF to think about how the standards that already exist interoperate in practice, or the implementations of those standards, and how that goes forward when new standards are introduced.

So, yes, there is this mode where different organizations cooperate. Now, every end user can modify this software. That's the beauty, right? And then you can also destroy the interoperability by making changes that breaks things. So, yeah, there's also the freedom to shoot yourself in the foot. In practice, I think the maintainers of this software are quite concerned about interoperability, because that's what makes the internet and DNS work. I hope that answered your question, and otherwise I will defer to Tuesday, if that's okay.

JONATHAN ZUCK

All right, Kathleen Scoggin is next.

KATHLEEN SCOGGIN

Hi. I have two quick questions. The first one is slightly more technical. Don't kill me, Jonathan. But I was wondering about the decision to categorize the research as FOSS versus OSS more generally, given some of the debate in the community, and what that would mean for messaging the report.

And my second question was, I guess, on the topic of how the At-Large can help more generally, is the goal of this sort of collaboration and speaking about this to message the report for increased maybe like a confidence-building measure for end users of the security of the DNS? Or kind of what is maybe the collaboration between us and place we can be most helpful? Thanks.

MAARTEN AERTSEN

Thank you. I'll go to the second question first, if that's okay. So, what I think is very powerful about the end-user perspective and the way you come together here is that you have a global reach. And in the end, a publication like this that documents a technical reality is only useful if it reaches policymakers as they decide how to regulate or how to shape new laws, etcetera.

So, it's not as much that this report is relevant to end users because they need to read it, it's relevant to end users because they live somewhere. And it might be the case that in the future, where they live starts to regulate software or critical infrastructure in a way

that impacts this development model. Your first question was around terminology, so Open Source versus free software.

So, there is a bit about this in the report, and I'll refer there. Free and Open Source software is a term that basically encompasses both communities, and that's why we use it. But there's books written about the differences in perspective, and some people are very passionate about it. We picked a term that seemed least controversial, but I'm sure there will be people who would have preferred us to use a different one. Thank you.

JONATHAN ZUCK Matthias is next in the queue, please.

MATTHIAS HUDOBNIK Thanks.

JONATHAN ZUCK And I think Alan, and then I think we close the queue.

MATTHIAS HUDOBNIK Thanks, Jonathan. Matthias Hudobnik speaking for the record. Actually, I just wanted to echo once more on this end-user perspective. I mean, as we already talked in the morning, I think the most obvious thing is to talk about it, be aware of it, and then also advocate for it if you like it.

And the RALOs are the perfect place to influence also in your region. And I think this is the first good starting point, because most of the people, it's a complex topic. Most of the people might not even be aware about the DNS, and then take it from there and try to influence and talk and also spread the word about it. Thanks.

JONATHAN ZUCK Thank you. Alan, please go ahead. Yeah.

ALAN GREENBERG Thank you. I'm responding to Kathleen. In your country or my country, we may have very little real opportunity to influence the policymakers. For many people around this table and in At-Large, the distance between our participants and policymakers can be very, very small. In many small jurisdictions, there are not a lot of technically savvy people, and that connection is strong and short.

So, I'm not sure that we're looking as much for an end-user perspective as an ability for our community to help influence the direction where this is going. Thank you.

JONATHAN ZUCK Yeah, and I don't know why I couldn't sit down with Donald Trump and talk about free and Open Source software. I think that would go over very well. But I didn't mean end-user in the way we normally use it. I just mean like, in other words, it's At-Large community. What is it that needs to get communicated to policymakers? Just the fact that this is the case or that they are at

the precipice of doing things that might undermine it? What is the talking point that needs to get delivered? That's really what I meant.

RAM MOHAN

Could you go two slides prior? Maarten, I wonder if this is not the main education and understanding we want to make sure is communicated. When regulators apply a software bill of materials or attempts to regulate software looking at a supply chain, it may not exactly work when it comes to critical infrastructure.

MAARTEN AERTSEN

Yeah, I think that would be one way to do it, Ram. If you live somewhere in the world and you hear of this report through your radio, for example, what the action is, is to remember it once you hear of impending regulation on software. And at that point, it might become useful because the report documents other regions where they've been through this exercise, where there were stakeholder conversations, and where they landed in a place that is not damaging, but in some cases even strengthening how this works.

And it starts with recognizing that the software space, especially for the internet, is very, very different from the physical space of physical objects where you maybe buy something like a children's toy in a store, and because we want safe toys, there is this regulation which makes everyone in the supply chain in some way

responsible for that safety. And that approach seems very nice, but doesn't work if there are not such contracts, etcetera. And therefore, whenever software is regulated, it makes sense to make sure those that are regulating know how the internet works. Yeah, I hope that's--

JONATHAN ZUCK All right, thank you. This is a great report, and thanks for sharing with us, and we'll work through it together, and we'll figure out the incidences where we can be helpful with it. Oh, you didn't hear the part about me closing the queue. Is that what you're saying?

Do you speak English, sir?

OLIVIER CREPIN-LEBLOND If you have 30 seconds.

JONATHAN ZUCK 30 seconds, that's okay, that's enough.

OLIVIER CREPIN-LEBLOND Olivier Crepin-Leblond speaking. I'm sorry for not paying attention. No, just to add, I think that it's also important in light of what's happening these days when there's a significant amount of lobbying from commercial firms that try to sell you their ware and say, our propriety system has got guarantees, etcetera. This Open Source stuff is not good enough. I think it's extremely good to

remind governments in particular that Open Source is extremely good and actually sometimes better than proprietary.

JONATHAN ZUCK All right, let's go back to the agenda and move on. I think we want to hear what else you're working on.

RAM MOHAN Yes, thank you. So, let's flip three slides over. There we go. So, this is to give you an update on not just current Work Parties, but also upcoming Work Parties. Next slide, please. So, one Work Party that the SSAC has just chartered a little while ago and has begun work on is what we call RIDE, the Responsible Integration into the DNS Ecosystem. This is a Work Party that is focused on new technologies that are evolving in the identifier space.

There are technologies in the blockchain space, for example. They call them blockchain domain names, even though they're not domain names in the way that they are defined. But there are identifiers in the blockchain space. And so, we're looking at identifying clear guidelines that can enable new technologies like those to integrate responsibly with the DNS system that we know, that we depend upon, that we rely upon, and that has characteristics and qualities that are well-defined, right?

So, our intent is to make sure that the security, stability, and especially user trust, end-user trust, in not just the identifiers, but in the ecosystem of identifiers is not diluted because new

identifiers are arising. And new identifiers are not only arising, but new identifiers are arising that borrow the same nomenclature of the well-known and established DNS ecosystem that we know of, right?

We call domain names, we call resolvers, and in the Web3 infrastructure, you find terms that are the same, but they actually don't work the same or do the same thing. End-users are not going to be expected to understand the difference between these things.

So, the key areas of study are the domain life cycle, user confusion, particularly there, the focus is on preventing fraud when similar names exist in the DNS ecosystem, domain names, for example, and similar names exist in new namespaces, right? And from there, we intend to provide some analysis of the risks that could be introduced to the DNS itself, but also to the users of the DNS, the end-users and other users of the DNS, right?

So, this matters in our perspective, particularly for end-users, because our aim is to ensure that the domain name system remains predictable, reliable, and trustworthy. We want to acknowledge and embrace the evolution of technology and innovation that happens in the technology space, but we, at the same time, want to make sure that the foundations of predictability and reliability, stability remain. So, that's the first Work Party that we're working on. I'll pause a moment if there are any questions about this.

JONATHAN ZUCK Wow, that sounds very relevant to us.

RAM MOHAN Okay, terrific. Let's go to the next one. This is a Work Party that is focused on DNSSEC Operational Considerations, and our focus here is to speak to, this is aimed a little bit more at audiences who want to, who think of deploying DNSSEC. It could be enterprises, it could be small businesses, it could be small organizations, non-profits, it could also be technical operators. And what we want to do is to demystify DNSSEC.

This entire area of DNSSEC over the last so many years has accumulated a continuing mountain of technical jargon and extremely dense technical material associated with it. So, we want to make sure that we can demystify it, and for internet operators, we want to make sure that they can deploy DNSSEC safely. There is some concern in some parts of the ecosystem that deploying DNSSEC may run the risk of having your systems become more fragile because of the many component parts that are there, right?

So, we want to analyze adoption trends and barriers, evaluate what are the tools that are in use, what best practices are being used today, and the internet is rife with many stories, many anecdotes of outages that arise from DNSSEC-related issues. So, we want to list all of those things, and at the end result, provide a report we're targeting in sometime early next year, a report that provides an analysis, kind of clear-eyed analysis of what are the benefits of deploying DNSSEC, what are the trade-offs, the pros and cons of

various approaches, real-world examples of deploying DNSSEC and mistakes that got made, right?

And a step-by-step implementation plan, if you want to deploy DNSSEC, what are some of the things you ought to be doing, what kind of investment should you be making, right? And how do you make sure that once you deploy DNSSEC, you don't have buyer's remorse, right? So, that's the focus of this Work Party. I'll pause again for any questions that you may have.

JONATHAN ZUCK I want to make sure there aren't any here. I guess I'll ask one. Have you given some thought to creating some kind of a landing page for particular actors that might want to, that might be the consumers of this information so that it's less because part of what we might be able to do through our employers and academic connections to IT departments, et cetera, what that might be, is to drive people to some place.

I don't think we're ever going to be the people delivering the details of this material, but we can say, are you considering it and are you worried about it? And if you are, go here. I mean, have you thought about having a place where there's a video or a colorful manual or myth busters or something like that that we could be a part of driving people to?

RAM MOHAN

Yeah, we had a discussion about it. We had a Work Party meeting yesterday and that was part of the discussion. How do we disseminate this information in a way that is technically accurate without being technically dense? And we were talking about maybe a little short video or other materials like that. So, that's in the plan. When we finish the report, that's part of our thinking. So, thank you for that. Next slide, please. Oh, sorry, please.

AFTAB SIDDIQUI

Hi, Aftab Siddiqui. Ram, one question I have. Is this the work you have mentioned, the outcome you're looking for? It is the extension of the OCTO 29, which the ICANN Org did in the past, which has all the three points you have mentioned in detail. It's been there for four years. We have used that document quite extensively, at least in the Asia-Pacific region. So, is that the extension of what was done in the past or this is totally new work?

RAM MOHAN

It integrates some of the work that has been done, but the real focus here is to look at what the design parameters are, when you want to deploy a DNSSEC, what are the risks that you have to consider, and what are some of the benefits that you get as well. So, we look at this as something that complements the document rather than extends that document. All right, last slide.

We have two new Work Parties that are kicking off relatively soon. The first one is to examine AI's role. And we say AI maybe it's AI,

maybe it's ML. We have to define that more clearly. But the role of those technologies as an emerging tool for both executing sophisticated attacks as well as a tool for better detection and mitigation techniques.

Now, we've come and spoken with you before about AI and DNS Abuse in prior sessions, but that was a little bit more, at that time, an extension of lightning talks that we had from within the SSAC. This is a kind of a dedicated Work Party. We're just in the process of building the charter of this Work Party.

And the thing that we're trying to resist is the temptation to just AI-ify everything, right? Just stick that word to whatever, and suddenly you'll have more clicks or more whatever, right? So, we're trying to make sure that it stays within scope, within the focus of the things that both the SSAC has chartered to do, but also where the SSAC actually has expertise to bring to bear, right?

JONATHAN ZUCK You know that you can use generative AI to make the paper more likely to get clicks based on the, you know.

RAM MOHAN Yeah. And we thankfully are a committee that doesn't measure success by number of clicks. The second Work Party that we've just built the charter and we are getting going is, we're calling it DNS transparency, but the real issue underneath is to explore the benefits of faster zone file, domain name zone file updates,

potentially all the way to a live feed of all newly registered domain names.

And that's because we've had some of our security experts identify that there is a potential new class of, or maybe not new, but there's a class of threats that happen. We're internally calling it transient domains. These are names that are registered and are used for a malicious purpose, and they go away between the time that a zone file is published publicly, right?

So, if you're a security researcher and you want to look at what's going on, that domain vanished. It never existed, even though for its lifespan, it did damage, right? And so, we're looking at exploring that, understanding that better before we can come to any conclusions. Comments, questions? Is that a new hand or an old hand there? Oh, okay.

KATHLEEN SCOGGIN Hi. I just have a quick question. I know that both you and the GNSO are at the beginnings of scoping a lot of things about DNS Abuse, and so I just had a question. I was watching the GNSO earlier, How This Work Party would kind of differentiate its work from what's being done in kind of the scoped PDPs there?

RAM MOHAN Yeah, unlike the GNSO, we have no power. We merely render advice, and we hope that the value of the advice is sufficiently compelling that it gets adopted, right? That's one part. But the

other part is that we're not looking to affect policy changes or affect contractual other changes as of yet.

The work here is much more to provide a clear look at what the emerging kind of state of the art is, and to present that, and from there, hopefully, that will educate or inform folks who want to make policy or want to make operational decisions. They can go from there. I hope that answers your question.

KATHLEEN SCOGGIN

I have like a tiny follow-up, if that's okay. I guess just since it has, I feel like, been recognized, at least by the CPH, that this is an issue, or the whole conversation that we had around bulk registrations, etcetera, which has now shifted to other names, but has recognized this as an issue. Yeah, whatever that is. And so, I guess just if there are other kind of subtopics to this that would be important for us to know and us to communicate back to end users outside of what has kind of already been established.

RAM MOHAN

Thank you. Completely on point. And we look forward to being invited into that policy development work and providing our thoughts in that area.

ALAN GREENBERG

Thank you. The second one fascinates me. How do the domain names disappear? And is this yet another form of domain tasting

with a different rationale? And is it using the same mechanism? I said disappear.

RAM MOHAN All I meant is that it's, can you observe it, right? Because if you have, for instance, a zone file that is updated, publicly accessible and updated, say, every three hours, and if you have a domain name created on the first minute after that last update, and if it's deleted at the 90th minute, right, from the zone file update in minute zero to the zone file update in minute 180, that domain name won't even appear.

ALAN GREENBERG No, I understand that. My question was, how does it get deleted in that time frame?

RAM MOHAN It's pretty simple, right? You can go to a registrar and you can ask to create a domain name and you can ask to delete a domain name.

ALAN GREENBERG I guess I didn't realize that the user can cause it to be deleted on that time frame.

RAM MOHAN Russ, do you want to speak to it?

ALAN GREENBERG Probably a registrar can find it fast enough and delete. I know the registrar themselves can do it, but that goes back to registrars complacent, not complacent, involved in the process, which is a different issue. And maybe we do need policy on that

RAM MOHAN And we're not going to speculate on that here, but we do, if you look at NetBeacon, for example, and some of the reports that they have provided there are some examples that exist about over-indexing and things like that. The thing is that when you have API-based systems and automation, it's fairly easy to do those things without the awareness or knowledge of parties in the middle.

OLIVIER CREPIN-LEBLOND Yeah, thanks very much. Olivier Crepin-Leblond speaking. I think that there's probably a semantics out of it. You mean deleted. Do you mean the registrar deletes the whole domain name, or do you mean it gets deleted from the DNS? These are two different things.

RAM MOHAN Well, we're talking about zone files here, right? When you look at systems and you're a security researcher and you look at it. You're analyzing the zone file, right? So that's the view rather than the database, the domain name database view.

OLIVIER CREPIN-LEBLOND Yeah, it's Olivier speaking and that's exactly the point. It can be deleted, added or deleted from the DNS as and when by the end-user actually. Thank you.

RAM MOHAN Okay. That covers the current and upcoming work, let's go to the next slide. This Jonathan, we said we may not have enough time to cover, so why don't we skip this and go to the next piece? And I'll hand it off to you, Avri.

AVRI DORIA Thank you. I was hoping you'd spend lots of time in the one before it. Okay, Avri Doria speaking. So, I want to really get a discussion going here. Now, what I've done twice so far to the poor folks in ALAC was and go through and I'm going to ask to display it the next is the purposes of doing reviews and if somebody could put that up.

And what I've done is, we've talked through them and people have given a couple places where they see issues, words here, concepts there, that need to be added to it. With the 15 minutes that we've got here, though, I was looking more and I was really hoping to get more from Jonathan, and Robert if he was online, and Suzanne, who's in the room. But from all of you into one of the questions, is it possible to put them up so that anybody that hasn't read it could?

So basically, yeah, that's you know, so the purposes. Yeah, it's nice, it fits in one screen. These are the purposes, I've gone through them several times. I'm starting to bore myself almost. I'm

probably boring the folks from ALAC that have already heard it at least twice.

So, I really wanted to more look at it. I'm sure you've all read it. If not, you can read it within 13 seconds. Is, one of the questions we will be asking at the session tomorrow and we have several questions. It's a Mentimeter, but it's also one that we asked at the prep week session; is, are we heading in the right direction with this analysis? Are we headed in the right direction with the purposes as being laid out, leaving aside that there are certain places where we need to be more inclusive?

We need to include looking at more of some of the issues dealing with structure, substructures, components and interactions. We've had comments about the bottom bullet in a) of, ICANN duly takes into account public policy advice of governments. Heard earlier about SSAC mentioning, you know, well, we hope-- and this was on a technical issue mind you-- but we hope that people listen to our advice. I've heard similar things from ALAC is, we hope it duly takes into account our advice.

So, you know, are bullets like that heading in the right direction? When we're looking at Continuous Improvement Programs in b), and not looking anymore at the old traditional operation reviews or organizational reviews rather. There's no mention of operational reviews of ICANN, but that's a different issue. Are we asking the right questions? Are we looking at the proper reviews? Are we doing the right thing?

And so, I'd really like to ask, and of course going to people like Jonathan and Suzanne, you guys have been listening to this already quite a bit, so perhaps you could start it off, but as opposed to me going through each one of these, and trying to explain the words behind it. Does anybody want to speak up about it?

MICHELLE DESMYTER Robert's hand's up.

AVRI DORIA Robert's hand's up. Robert, please.

ROBERT GUERRA Sure. So thank you, Avri. I think one thing I want to just take a step back, because you just went straight into it, which is perfect. But just for everyone who isn't familiar, the review of reviews is in its fact-finding stage. And at this moment is that we've had discussions internally with the group members and we've laid out, and this is what Avri's laid out is, these are the assumptions that we want to make sure are correct before we go into our next stage.

And so, we really want to appreciate and get feedback from everyone. Because we have a very tight timeline, we want to make sure that these items are correct and encompass-- and the assumptions are correct before then we get into a lot of work. And so, please review them whether they're fine, there's some

additional language that needs to be added, this is the point to do so, because then forever hold your peace.

AVRI DORIA

Thank you, Robert, except for that last line. This is ICANN, there's never forever hold your peace; at least I don't believe in my 20 years or so of hanging out here that I've ever seen it. But it really is important to get these right because I certainly do direct the rest of the years' project in terms of doing this and getting your statements in about these at tomorrow's session or within the next week, is very important because it does set the path going forward.

So I very much appreciate, Robert, pointing that out. It is important that you speak up to these. Forever hold your peace, if anybody can handle that out, that'll be interesting Please, Suzanne, thanks.

SUZANNE WOOLF

If I can chime in. Thanks, Avri. For me at least the kind of input I'm looking for as one of the SSAC-- Robert and I are the SSAC representatives to the Review of Reviews-- and the reason why I was interested in being part of the process is that we actually have a significant variety of different groups in the ICANN community with different roles and responsibilities.

And one of the things that always struck me about the previous history of review processes is, it never quite felt like the balance between a Generic attempt to evaluate and tailoring reviews to the specific group or activity never quite felt like the balance was right.

That's one of the things I'm very curious about, is where do people think those lines should be drawn where? To what extent does one size fit all and do we have? Consistent goals that always have to apply to reviews and to what extent do they need to be tailored to the specific group or activity?

And again, we have a fairly tight timeline and we have two open sessions this week, Monday afternoon, Thursday afternoon, but also a number of other discussions with different constituencies because we do need all the input we can get, we do need the guidance. Thank you.

AVRI DORIA Thank you. Jonathan, and then Ram. I don't know which came first, but Jonathan came first. So, Jonathan, please.

JONATHAN ZUCK I will say that the egg came first before the chicken. I don't know if that's relevant. Anyways.

RAM MOHAN You're calling me chicken?

JONATHAN ZUCK One of us had to be. One of us had to be. So, Susan, you raised an interesting question because it almost sounds like you're entering into the Continuous Improvement territory when talking about that, and I think that's where one of the exercises that we have in

front of us of maintaining that distinction between those two is going to be one of the challenges that we face for sure, given that we will potentially be designing a review of the Continuous Improvement Program, but not necessarily creating organizational reviews that the CIP was meant to replace.

Because I think going into this was this assumption that the ATRT3 recommended CIP replace organizational reviews and that that process is kind of working, but that this Pilot Holistic Review kind of fell apart and that led to this well-thought-out and honorable endeavor of a review of reviews.

So, I feel like the role that I've been trying to play on this is kind of a squeaky wheel. And I don't always know whether or not I'm, whose water I'm carrying when I do it, but I do have a sense that different organizations within ICANN might have somewhat different goals from this activity. And so, I'm always trying to make this document as expansive as possible and looking for things that it might not cover.

So one thing I raised is if, if the idea was that we wanted to have, for example, a review on whether or not the ICANN community is doing enough on DNS Abuse. I raise that as an idea, right? And people immediately said, well, you're going to mix things that are happening, the Contracted Party Houses doing themselves, things that are policy, things that are contract compliance, that there's all these things. But then it occurred to me, that's exactly what the Security and Stability Review did.

And so, but we're a green field here, so we shouldn't be limited by what went before. And so, it all becomes a little bit of a circular argument, but it seems to me that that was a valuable thing that the Security and Stability Review was doing, was something that was some umbrella level that looked at all these different areas. And so, I worry sometimes, as we get more enumerative in this document, we're finding ways to prevent that kind of umbrella review from happening. And that's why I'm a little bit of a squeaky wheel about that.

AVRI DORIA Thank you. I've got Ram, and then I've got Sebastien, and we've got four minutes.

RAM MOHAN All right. Well, since you called me chicken, I know how to cross the road and talk. But one of the things I just wanted to say is that from my point of view, it's a big undertaking, and Avri and the other co-chairs, you have a big job ahead of you.

You've set an aggressive schedule, and I just want to make sure that we acknowledge from the SSAC point of view that you have a schedule and that you have set deliverables and there's some accountability measures that are built into what is intended to be the big accountability thing, right? So good job doing that, and all the best on executing to the timelines, even if you don't exactly

meet the timelines, having those goals helps measure how it's going. So well done on getting that off the ground.

AVRI DORIA

Thank you for that. We were given the timelines and we're trying to meet the timelines that we were given. So, thank you for the thank you on that one. But yeah, we'll see how we do at the end. Sebastien, please.

SÉBASTIEN BACHOLLET

Thank you very much. I wanted just to underline what Jonathan said, that the Continuous Improvement Program was supposed to be outside of the goal of the discussion. I heard some questions about people who wanted to go back to the organizational review. I just want to try to remind me and remind you that if you look carefully to ATRT3, it is written that if a group considers that they need to do the Continuous Improvement Program in a way that it was done as an organizational review, it's still possible.

It's just you can have an outside consultant to do the job for you. Therefore, I am a little bit surprised when people say we need to revert to because for a lot of other groups, it's good to go in the Continuous Improvement Program. And sorry to take this common meeting for asking something for At-Large, but if we could have this document on Google Doc and put all the comments we had all together, it will be a good way to enhance the communication

between us and to work on that for the next few days and maybe later on. Thank you very much.

AVRI DORIA: Okay, thank you. Good suggestion. We have one more? One more minute. Yes, I could tell we had one more minute. And I don't see any more plaques up or people requesting. So thank you for those comments and for doing something better than me going through the list. And I pass it back to the two chairs.

JONATHAN ZUCK: All right. I'll take the home field advantage here and say, thank you once again for the SSAC for joining us, and as we went through those future work groups that you're planning, I see a lot of opportunity for synergy and a lot of real direct end-user related issues, and so let's find a way to prevent what I've coined as the dissertation problem of the SSAC. So, we're on board to do that and let's figure that out. Thanks for coming

RAM MOHAN: Great. Thank you for having us and look forward to more collaboration. Appreciate it.

[END OF TRANSCRIPTION]