ICANN84 | AGM – Joint Session: ICANN Board and SSAC
Tuesday, October 28, 2025 – 9:00 to 10:00 IST

WENDY PROFIT

Hello, and welcome to the joint meeting of the ICANN Board and SSAC. My name is Wendy Profit and I'm a participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Interpretation for this session will include English, French, and Spanish.

Please observe the following guidelines to participate in the session. I'll also post this in the chat for your reference. This is a meeting between the SSAC and the Board, so we will not be taking questions from the audience during the session unless we have time at the end. For remote participant members of SSAC, if you would like to speak during the session, please raise your hand in Zoom, and when called upon, virtual participants will be given permission to unmute and Zoom. On-site participants will use a physical microphone to speak.

We have a roving mic here at the table. Please state your name for the record when you speak, the language that you will speak if speaking other than English, and speak clearly and at a moderate pace. I'll now hand the floor over to ICANN Board Chair, Tripti Sinha.

TRIPTI SINHA

Thank you, Wendy. Good morning, everyone. Good day, everyone. This is first bilateral meeting for today. It is between the SSAC and the Board. We look forward to our interaction. On behalf of the Board, our colleague, Jim Galvin, will facilitate this meeting. Jim, over to you.

JAMES GALVIN

Thank you, Tripti, and thank you to everyone who has joined us this morning. Just a reminder, it is an open session between the Board and the SSAC, and I do want to encourage that any SSAC member or any Board member who would like to speak is open to do that at any time. There is a roaming mic that is available if you're out in the audience and not sitting at the table, but I do hope that we can get an engaging, interactive session going here.

So with that, let's just jump right in to our agenda. I understand that SSAC had three issues that they wanted to go through for the Board, and I will turn that over to you, Ram, for the first one.

RAM MOHAN

Thank you, Jim and Tripti, and thanks for having us. It's always good to come back and have a conversation with you. We have on the next slide, you'll see we have really three items to share with you. We don't have any asks in the traditional sense of, you know, we're coming and complaining to you or asking you must do this or that, but we have information to share.

So first off, let me throw the microphone over to you, Maarten, who is the chair of the Free and Open Source Software Work Party. We published a report on that just a few weeks ago, and we'd like to walk you through some of the highlights of that report over to you, Maarten.

MAARTEN AERTSEN

Good morning, everyone. My name is Maarten Aertsen, and I was co-chair of the work that looked at the software side of the DNS in this world. I'll be taking you through the report at a high level. So let's see. Next slide, please. And next slide, please.

So if you summarize the report in a single sentence, we found that the DNS is built and sustained on free and open source software. That's not advocacy. It's not us saying that that's better. It's just a statement of fact of how this infrastructure is actually built today. Next slide, please.

So what is free and open source software? It's not free as in you don't have to pay money. It's about freedoms. So this is software that is licensed in a way that allows for anyone to use it for any purpose, anyone to study it, including source code, to share it and redistribute copies, and finally, to actually change it even before you share it. So what this allows is it creates a fundamentally different ecosystem for development, distribution, and maintenance of software as compared to a proprietary model. Now, there's some philosophical differences about whether you

call this open source or free software. We picked the term that encompasses most of this by calling it FOSS. Next slide, please.

So SSAC, we look at risks to the naming system. So we also looked at risks for FOSS. So most FOSS in the world relies on single, unpaid volunteers. They might be experts, but if you're a volunteer, motivation is a critical factor, right? So if you lose that motivation, then there's a corresponding risk of burnout and project abandonment. FOSS is also different from proprietary in the sense that if you just download a copy as an operator, there's no warranty attached. So an operator must take responsibility for the software they run, and if they want support, they'll have to contract that separately because it's not part of this license, right?

Now, if you look at this from the organizational side, where it's not volunteers, you have the risk of funding because everyone can use this software without paying, and there is this free rider phenomenon. So the goal of this report in general is to educate policymakers around the world about how this infrastructure works. And so when you look at regulatory initiatives, the risk that is always there is that a regulatory burden introduces a funding shock to the existing model.

So these risks are real, and they are inherent to this model of freedoms attached to software licenses. But there are also trade-offs for strengths. So if we look at those strengths, next slide please, there is this notion of transparency and collaborative security. So the academic and operator community maintain quite

a strong and active culture of openly scrutinizing DNS software. And this has been going on for decades, where academics find issues either at the protocol side or the implementation, that's what we're talking about today, they bring it to the developers and things get fixed. So flaws in that sense are openly discussed and quickly fixed.

And when we surveyed operators for this research, they expressed that they really appreciate the ability to diagnose, verify, and expedite patching of vulnerabilities, because this supply chain is transparent, they can move as fast as they want, they're not held up.

Now what is different about the DNS, and it's somewhat exceptional if you compare it to FOSS in general, is that the most popular server software is actually maintained by long-lived and dedicated maintenance organizations. Most of them are in existence for more than 20 years, and they found funding models that work, even though they might not be in there for profit. So that's a big difference when we look at the DNS as opposed to FOSS in general.

Now another big strength is because there are these multiple organizations maintaining the software, and they produce multiple implementations, there is a diversity that can give operational resilience in practice. So if there is an issue in one implementation, an operator can still use the other one and avoid a single point of

failure, or economically speaking, a vendor lock-in. Next slide, please

So in summary, talking about security, it's not better or worse, it's different. So it's not so much about whether the source code is open or closed, it's not about people getting paid or not, it's not about it being commercial or non-profit, what really matters is the quality of the development process, whether there's review and rigor in testing, etc. So a quote from the report is that the security of any software project is determined by the quality of its development and maintenance processes, not the visibility of its source code.

So if you ask is FOSS more or less secure than proprietary software, the answer is it's neither. It's just a different risk profile, and that is a challenge in policy, because you cannot copy and paste regulations that work in a proprietary world and expect them to work in this radically different environment. Next slide, please.

So let's talk some data, because we made this single claim, right, that this is everywhere. We surveyed the root server operators based on the statements that I had previously published, or when there was missing data, we contacted them, and at least 9 out of 12 root server operators use FOSS exclusively. Now if you look at the ones that don't, they have this hybrid model where a FOSS implementation might serve as a backup. So this is not a small percentage. Next slide, please.

So if you look at the top level domains, we looked at the top TLD providers by the number of TLDs they serve, and if you combine gTLD and ccTLD, that's on the left, we find that 9 out of 10 use FOSS in their DNS infrastructure. If you focus on country codes, it's 20 out of 25, and if you leave out the IDNs, it's even 23 out of 25. Next slide, please.

So let's look at registries. So here's two models. The first model is where it's entirely FOSS, and this illustrates that it's possible to do this, like have a completely end-to-end open source registry, and examples here are FRED by CZ.NIC from the Czech Republic, but this model is possible, but it's not the most popular one. The most popular one is the second model, which is a proprietary registry.

However, when asking them, it turns out that these are not custom-built systems. These are custom-built systems, but they are not built from scratch. They are proprietary integrations built on top of a foundation that is overwhelmingly FOSS. So if you look at a registry as a database, we see registry operators mentioning database software, web server software, application servers, monitoring tools, etc., etc. So we found that out of the 10 that we asked, which are major registry platforms, all of them incorporate FOSS components. Next slide, please.

So the resolver infrastructure was the hardest to measure, but here we find that FOSS has a substantial presence, and our approach here was to look at what's available, not so much to measure what's being used. If you look at the query volume, 80% of users

use their local resolver, and here it's predominantly FOSS. Why is that? Well, it's either the existing resolver software or its commercial solutions, and in those commercial solutions, in the products that we looked at, usually it's FOSS inside. So you'll find tables in the report that illustrate this.

Now, the remaining 20% uses public resolvers, and here there's proprietary ones, but there's also ones that are running on FOSS. So we have Quad9 and DNS4EU. And Cloudflare, which we have a little case study on, is proprietary in the core but surrounded by FOSS. Now, there's a lot of cloud platforms, CDNs, hyperscalers, etc., and we find that at least four of those rely on FOSS. Next slide, please.

So that concludes the statistics portion, but we find on the whole that FOSS is the foundation of critical DNS infrastructure if you look at these numbers. Now, why care about all of this? Next slide, please. Well, there are countries around the world that are regulating software. They are regulating development of software or they're regulating critical infrastructure use of software. And when you take a traditional approach, you assume that there is a vendor customer model that assumes financial transactions at every step. But software does not have an inherent material cost per additional copy, so it can be provided at a near zero cost, and in the case of FOSS, this breaks the whole model of regulating a supply chain via contracts.

Now, in the FOSS reality, there are no guaranteed vendors or contracts unless an operator chooses to have them, so imposing compliance burdens on either volunteers doesn't work. And if you impose these type of burdens on small maintenance organizations, you could threaten their source of funding. So, how does that backfire? Well, then you would see maintainers abandon projects, switch to proprietary license, or avoid regions, and the software we depend on becomes less available and less secure. Next slide, please.

So, the report includes a number of case studies of regulations around the world. I will not dive into these today, but the point here is that there are FOSS-aware policies, and when additional parts of the world start on this path, they can learn from these. So, these are positive examples, and we had a look at them. Next slide, please.

We conclude the report with five actionable outcomes for a policymaker audience. So, first, they should explicitly recognize that critical infrastructure relies on FOSS. They should consult when they make regulation in this community. They should make use of the contemporary cases that are available, and what we see in one of these contemporary cases is to incentivize the sustainability of this model.

And finally, it's important to address systemic risk collectively. So both in the proprietary and the FOSS world, we have a lot of dependencies on critical components. It's not unique to FOSS, but

that's a problem that needs to be addressed. Let's see. Next slide, please. Key takeaways. The DNS runs on FOSS. FOSS is different, and we can get this right. Now, final slide, please.

This is not part of the report, and it's more of a reflection, perhaps for discussion right now. There are pathways for ICANN to take. So, we can acknowledge this reality. Government engagement can use its existing work and network to signal where software regulation is emerging and then surface our research. And finally, the community has already recognized the role of FOSS in its recommendations that are at the basis of the ICANN grant program.

So, that's it for my quick run-through of the FOSS presentation. If you like this a lot, we have a longer version this afternoon, though I know you will not have the time to attend it. I guess there will be a recording. So, I'll give the mic back to Jim, and thank you for your attention.

JAMES GALVIN Thank you, Maarten. I appreciate it. I will say on behalf of the Board that this particular report has been very well received and has garnered a lot of interest from a number of Board members. But let me turn it over to David to kick off our conversation and response here about this. Thanks.

DAVID LAWRENCE So, hello, David Lawrence. Many of you, some of you at least, are probably aware that my career on the Internet actually started in

the open source community. I first was at the Free Software Foundation before moving on to the Internet Systems Consortium, which famously rewrote the BIND name server to BIND9, and I was one of the co-authors on that project. So, I am delighted to see that you view the DNS software ecosystem to be healthy.

The one question I have as was going through was what more can ICANN do? You're aware certainly that ICANN has an annual domain name DNS Symposium, and there are also other groups like DNS-ORG and, of course, the ITF, which many of the open source contributors actively participate in, and that includes ICANN staff members in each of those forums.

And so, what was interesting to me on the very last slide, you said one thing that you'd like ICANN to do is to acknowledge the importance of FOSS. And I guess my one question is, apart from the publication of SAC-132, what form do you think that acknowledgement should take?

MAARTEN AERTSEN So, this report is maybe a bit of an atypical SSAC report because it's targeted at policymakers outside of the ICANN sphere. It is targeted towards people that make laws, and we know that we do not reach them directly. So, maybe like the DNS blocking paper before this one, the power of this paper will be to put it in the hands of the people that do talk to lawmakers. So, in terms of what is the value of acknowledging, I think it is to put this work in the spotlight

for a future where there is regions of the world regulating this space.

We've seen a number of them. The US has made its vision in the past. The UK has done something. The EU is furthest, and there the discussion is basically done and ended positively from my perspective. But there will be others in the future. So, acknowledging, I think, is positive in the sense of supporting these existing venues where there is lots of cooperation. But I think it's even more important to acknowledge it at the point where people start regulating. And I think then ICANN can have a voice to surface our research. I hope that answers.

JAMES GALVIN Tripti?

TRIPTI SINHA Maarten, thank you very much for the presentation. This is excellent work. I don't think I've ever seen something like this done before. I have a question on slide seven. If you could go to slide seven, please. In the middle section, it says the stability of core DNS projects. They use FOSS, and you say they have a sustained funding model. Could you speak at a high level what the nature of those sustained funding models are? You did say they're not profit-driven, but they are sustained funding models. So, it's interesting. I'd like to know how they achieve that.

MAARTEN AERTSEN

So, the four organizations that we've treated in the report, based on the statistics, are each quite unique. So, there's ISC in the US, there's CZ.NIC in the Czech Republic, there's my daytime employer NLnet Labs in Amsterdam, and then there's PowerDNS, also based in the Netherlands, which is a company. So, each of them is unique. My personal perspective is that it's also, like, first of all, it's due to the persistence of the people that have worked there that they have been able to survive. I can't speak to the specific funding model of, for example, ISC. I know for us, in the beginning, it was just a pile of money, but that didn't last long. And then, nowadays, it is support contracts.

So, operators who run software of NLnet Labs have a choice. They can either invest in staff expertise to be able to diagnose and fix software when they encounter really weird behaviors, or they cannot do that and contract us to be able to be their second line, to ask questions, to ask for a patch. So, PowerDNS is a commercial company. I can't speak on their behalf, but I think they're in the business of even stricter SLAs, maybe even-- And CZ.NIC is part of the national registry of the Prague Republic. So, they are a bit bigger, and they also have a different model, but each is unique.

And in doing this research, what we observe is that if you make regulation, the fact that these organizations have been existing so long does not guarantee that they will in the future, right? So, if you cut off one of these funding models, which are unique, for instance, then things might go differently in the future. Yeah, we don't know.

But this was definitely on our minds when the EU started to regulate software.

JAMES GALVIN Thank you. Wes?

WES HARDAKER Thank you. I'm extremely happy that funding was included, I think, as a concern for open source. It's a constant concern for all open source. What my question is going to be, though, is technologies rise and fall over time, and the need for technology. And as a particular need for-- It's harder than DNS. I can't say that DNS is going to go away. That's not going to happen anytime soon, most likely, although the next topic is going to get to that a little bit. But I can imagine elements of the DNS going away, particular R types, or records, or usage of some kind going away. What I find in open source that is a real struggle is when that happens, the need for the technology far extends beyond the point where people are willing to pay for it.

So, as a technology is fading out, it gets harder and harder for open source software systems to find funding to continue to maintain and do the maintenance that is required. And I speak at length of it, because I've had to deal with that, but I'm wondering, did you guys have that as part of your discussion? It's also the long tail of funding, besides when it's easy to find when new technology is

coming around. Everybody wants to pay for it. It's very hard to find that long-term maintenance.

MAARTEN AERTSEN

So, thank you for the question, Wes. It's not all positive in that sense. So, this has main server projects, but there's also a few that are maybe not as lucky. So, one piece of DNS software that millions and millions of people rely on is called DNS mask, and it has been maintained for decades by a single individual in the UK, not being paid for it, but it's in cable modems, etc., all over the world. Another example is CoreDNS, and more specifically, the underlying Go library, is also maintained by a single individual.

And so, over time, this really depends on their motivation and their ability to make a living for all of us to have this stable system that we are used to. Now, your question was specifically about changes in technology, and I don't have a great answer for you right now, but I think funding is a part of this, about the ability of a project to adapt. In the end, even if you like it a lot, you will need red on the table. So, I don't have much more on this for you, but I think that is a piece of that puzzle.

JAMES GALVIN

Thank you, Maarten. Thank you to the SSAC. I'm not seeing any other hands. I want to read out a couple of comments that are in the Zoom chat room that I think are interesting. Robert Guerra just reminding us and adding to the government engagement bullet

item from you about a great paper for ICANN GAC capacity building, something to be included there in that work. And I will read out from Ray Bellis, which many of us here know from ISC, just pointing out that their funding, since we had the funding question, that some of it also comes from support contracts, and that's part of their sustained model. So, okay. With that, let's move on to the second topic from SSAC. This is about work party progress, and back to you, Ram.

RAM MOHAN Thank you, Jim. So, we want to brief you on two work parties that are currently underway and two that are just being chartered. Next slide, please.

So, the first one is what we're calling RIDE, Responsible Integration into the DNS Ecosystem. What we're focused on there is the increasing integration of domain names with new technologies like blockchain and other decentralized platforms, and the novel challenges that they present to the security and stability of the DNS. From our perspective, it is crucial to proactively address those challenges, to maintain user trust, and to prevent potential abuse.

Additionally, the work that this work party is doing is intended to complement work that is presently active in the IETF DNS op working group. Just to give you a little bit of context, the SSAC has in the past addressed issues related to DNS security and stability, but here what we're looking at are the specific challenges posed by

the integration of domain names with emerging technologies, right? So, while we've done work, and we'll draw upon that, we think there is other work to be done.

In particular, our focus is to discuss requirements and constraints for adapting other technologies to interoperate with the DNS rather than adaptation in the other direction. So, we're looking at it from an incoming point of view. And just to brief you, in the past, the SSAC has written about possible resolution impacts of alternate naming systems. We did that in SAC123. We've also published reports on the stability of the domain namespace in SAC90, and about private use TLDs in SAC113. But 90 and 113 deal with namespaces defined by the DNS root zone rather than with other possible resolution and naming systems.

So, that's our focus. We're going to study issues that link to domain lifecycle, to user confusion, and to security and stability. The work party has just been chartered, and Rick Wilhelm is the chair of the work party, and he's to add any further comments on this.

RICK WILHELM Thanks, Ram. So thank you for that overview. That's bang on, all of that very good context. As Ram said, what we're talking about here in this work party is if an application, most notably blockchain applications, are going to integrate with the DNS, here are some recommendations on how registries and registrars should accomplish that integration rather than thinking about how the DNS has to adopt to the blockchain applications. Perhaps it's

obvious, but we're writing this not only for registries and registrars, but also for other interested parties in the blockchain ecosystem.

One of the things that we here at ICANN often forget, but you remember as soon as you step out of the ICANN circles, is how much we know and how much we take for granted about the DNS ecosystem. And all you need to do is to go to another conference, which some of us do, about places that aren't as facile in the DNS or domain names. And you realize that knowledge of domain registration techniques, approaches, what the difference is between a registry and registrar are completely lost upon its normies, if you will.

And so we're going to be documenting those things and helping to educate and provide pointers to existing resources to summarize these things so that we provide guidelines to summarize ways that integration would be accomplished without compromising security and stability of the DNS, in summary. We're early on in the work party. We've just been writing. We took a bit of a detour because the work party provided a document to the comment process on the applicant guidebook that was published at SAC 130. We provided some emphasis to some existing comments in the NCAP report to provide guidance around to the applicant guidebook in that area. So we're in the writing stage and we'll be back in upcoming meetings to provide a summary on where we are. I think that's probably about enough. Thank you.

JAMES GALVIN: Okay. Thank you, Ram and Rick. We'd like to open the floor for some questions from others. Let me turn it over to Russ to kick off the discussion on behalf of the Board.

WES HARDAKER: Thank you. I think that the timing of this work in SSAC couldn't be more critical. I know, Rick, you and I have had discussions about the need for looking into this topic, so thank you to SSAC for taking this on. There are certainly multiple angles and multiple viewpoints to this subject. I think we've heard them all, and I'm sure the technologists in the room know that the technologists in the world are very good at disagreeing with each other or thinking there are different correct solutions to things.

Some of those discussions are occurring around namespace integration itself. How do we do it? Some are related to the new usage of the DNS. It's resulting in the DNS being used as is in new ways, but also possible evolutions to the DNS itself. How does the DNS need to change to accommodate some of these newer technologies?

I will highlight that there's a few documents out there already about that. An important one is RFC 2826, which is written in May of 2000, which is an IAB document that documents the importance of the unique namespace and how to prevent user confusion. We really need a unique way so that two people on opposite sides of the world can communicate about the same content, of which it's heavily based in the name system. OCTO has analyzed the

challenges in this situation in OCTO 34, and as was already mentioned, there's a responsible DNS integration draft being actively worked on in DNSOP right now.

So I think my starting question to SSAC is going to be, are you planning on addressing the challenges in OCTO 34 specifically, but more generically in all the other documents I just mentioned as well?

RICK WILHELM

Thanks, Russ, for the comments and the questions. Thank you. Yeah, the IETF draft is sort of one of our-- anchoring documents is not really the right word, but one of the origins I think helped us in SSAC realize that we had a need to write about this, I think, because the IETF was actively working on this work, and we saw the need to sort of move in parallel to provide a comment from the ICANN perspective, because the IETF has its area of operations, which those around this table know quite well, and the SSAC as part of ICANN has a particular point of view and perspective.

And so it's important for the ICANN perspective to be brought into this discussion about the integration of DNS, but blockchain into the DNS, similar to the way that IETF is commenting on it. And so we view them as very complementary and not competitive. That's a very important thing, and thank you for bringing that up.

JAMES GALVIN Okay, thank you. I'm not seeing any other hands or comments, so let's move on to the next topic. Ram?

RAM MOHAN Thank you so much. The second work party from the previous slide that we're also working on is on DNSSEC operational considerations. This is not so much about whether DNSSEC is good for you or bad for you, things like that. This is really about demystifying DNSSEC, and the focus is on helping make sure that operators and people who want to deploy DNSSEC can do it in a reliable and predictable way. So our approach is to look at what's already happening in the DNSSEC namespace, if you will, what's happening with DNSSEC.

We're interviewing registries and registrars, both in the CC space and in the G space, to understand what kinds of challenges, what kinds of benefits they're seeing. Our intention is to publish a document that speaks, I guess in a very direct way, about the benefits of deploying DNSSEC, but also the trade-offs and the various approaches that can be taken. And really end with some practical step-by-step implementation pieces.

For instance, inside of the work party, we're talking about the fact that it may not be for everyone. DNSSEC deployment may not be for everyone, and organizations should make a considered choice on deploying DNSSEC. If they do make a choice to deploy DNSSEC, what are some of the base conditions they should plan for? What

kind of resources should they be planning to have in order to deploy and to operate DNSSEC going forward?

So our focus is less about the initial instantiation of DNSSEC in your zone or in your infrastructure. It's about keeping it running over a long course of time and understanding the trade-offs for that, understanding the benefits of that, but also understanding that it can, in many cases, be something that is a complex undertaking, and you have to make sure that you plan accordingly for it. So that's the intent of that document. I'll pass it back to you, Jim, for any questions.

JAMES GALVIN Thank you. I will make one comment while I look for folks who do want to comment. I think that, just as a reminder, ICANN's strategic plan, the upcoming next five-year one, carries forward from the previous one that ICANN has a responsibility to continue to promote the security and stability of the DNS in general. And historically, that has always included DNSSEC, and I like to frame it as DNSSEC everywhere kind of comment.

So I think this work by SSAC is important work because it's reframing that conversation and giving us a chance to think about that differently and the role of DNSSEC in the community and the ecosystem at large, and I do think that's important. So I see two hands over here. So, David, first.

DAVID LAWRENCE So I am curious to what extent SSAC has been looking into the quantum cryptography risks. As we know, this is an emerging area of technology that threatens traditional cryptographic algorithms, and it will have an operational impact. Has SSAC been looking at that yet?

RAM MOHAN We've had several lightning talks in this area, but for this work party itself, we have not ruled that in scope for what we're looking at. However, when we interview registries and registrars, it's entirely possible they'll bring it up as an area that needs to be studied.

JAMES GALVIN And Wes?

WES HARDAKER Thank you. So I obviously believe this is an important working group, and I'm an invited guest into it, so I'll disclose that. But I was once told to always admit what you don't know, and don't be afraid to say when you don't know information. I think one of the tradeoffs of running any large-scale important service is watching out for failure, right? Especially when there's a lot of people depending on it. So when you get to things like TLDs, we have an emergency fallback mechanism.

I kind of wonder if in this working group we should be talking about how do we deal with emergency help situations where we're not quite to the point where the TLD is completely failing and it's going

to be taken over by the emergency services that ICANN has, but how do we just help somebody get out of the critical failure path when they are struggling technically or struggling operationally for a short period of time because the DNSSEC imposes more time limitations than before. And thank you, Ram, your comments earlier actually triggered this thought in my head.

RAM MOHAN I think that's really on point, and we'll make sure to integrate that. I'm also happy that you're in the work party as an expert, so please remember to bring it in as well. Thanks.

JAMES GALVIN Thank you, Wes. Okay, not seeing any other hands or comments up. Let's move on. Thanks.

RAM MOHAN Briefly, there are two new work parties that are being chartered. The first one is on DNS abuse and artificial intelligence. In that area, what we're starting to look at is what is the role that AI has as an emerging tool for executing sophisticated attacks. Laurin, here to my left, is the chair of that work party, along with Matthias. So do you guys want to speak just briefly to that?

LAURIN WEISSINGER Hello. Yeah, so this is Laurin. Very briefly, because this really started to be discussed this week, so we're thinking a lot about kind

of like the impact of AI. But first, we are dealing with questions around definition, scope. All these kind of questions are currently under discussion in the SSAC. We will see where we are getting with all of this, and we're obviously happy to keep the community and the Board informed about what's going on.

RAM MOHAN Thank you, Laurin. The second work party that we're also just beginning is to explore the benefits of rapid zone updates. We've had a lightning talk inside the SSAC that has focused on, I don't know if I'd call it a phenomenon, but focused on a particular set of actions where domain names are created and then deleted before the zone file updates are publicly made. So in the space between one zone file update and the next zone file update, domain names are created, used, and then deleted.

So what happens is that as a researcher or somebody who is observing this namespace, those names kind of go invisible. And in some cases, those names, I believe right now the duration is about 24 hours. That's plenty of time to do damage. So we're looking at this to find out whether there are mechanisms that might enhance the visibility of these names. We're calling them internally transient names and to be able to better identify any harms that they may create. Questions?

JAMES GALVIN Not seeing any hands or comments. Okay. So, thank you. Let's move on to the next topic.

RAM MOHAN Let's go to the next slide. We don't have a whole lot more to just share, but for the benefit of new Board members who are coming in, just to give you one minute on, there are five keystone topics that the SSAC has a constant eye on and is constantly looking to work on and be an authoritative voice in that area. On the next slide, please. Those five topics are DNS abuse, new gTLDs, DNSSEC, alternative namespaces, and Internet governance, and the SSR aspects, the security, stability, and resilience aspects of Internet governance. So those are the five keystone topics that our intention is to not only pay attention but to build and develop an authoritative voice on those areas. So that really concludes kind of the SSAC topics part of this, Jim.

JAMES GALVIN Thank you. In this particular case, I'm going to draw on my joint role of being SSAC and ICANN Board and be the one to initiate some discussion here and ask some questions to bring this along.

SSAC, for the new Board members, SSAC has briefed the Board specifically on its five keystone topics. I do provide relevant updates to the Board technical committee as we go along, as I can. So, the Board is very pleased with this notion of how to organize the work into these five areas. And we are looking to sort of

understand, if you could say a little bit more about how you're making this work, how are you operationalizing this effort?

Obviously, I can see that part of the answer is the working groups. You have a couple of key working groups already in some of those five areas. But how are you going to measure success beyond SSAC's just publication of documents? Can you say any words about those two things, operationalizing and success components? Thank you.

RAM MOHAN

Thank you. One of the features of the SSAC is that it is an advisory body. It doesn't have any power, so to speak, which is a good thing because the weight of the work is what has to appeal for adoption. We're doing two things. Number one, we're starting to do some collaborations with the ALAC, with the Contracted Parties House. We just had a conversation yesterday with ISP constituency to take the content and to make it accessible to folks everywhere. We're going to start to do some of that work with the GAC as well in their capacity building. So we think we have a key role in that capacity building area. That's the first thing.

The second thing is we're taking the most recent documents, going back maybe 20 or 30 documents back, and our documents tend to be anywhere from 10 to 50 to 100 pages long and quite technically dense. So one of the big things that we're doing is taking them,

condensing them into 500-word plain English summaries that can be made available and more digestible. Thanks.

RAM MOHAN Okay. Thank you. I see a hand from David.

DAVID LAWRENCE On the five keystones, they very understandably have a focus on the DNS. I noticed an absence, at least for a number of resources being called out explicitly, although perhaps they were embodied in 0.5. And so my question is, does the SSAC concern itself with the management of number of resources, or is it considered explicitly out of scope, or how do the number of resources fit in?

RAM MOHAN They're in scope. We've written about that in the past as well. It just happens, David, that much of the inbound work that comes to us or other interest areas that come to us, there's a preponderance of it in the namespace rather than the address space. But we've written about that. It's in scope. I mean, the overall charter is about the identifier systems rather than the domain name system.

JAMES GALVIN Okay. And now I'm going to focus on one of the keystone topics and ask a particular question, DNS abuse, and ask that how does SSAC plan to contribute, be a part of the scoping discussions about the potential new PDP? And I do want to put for context here for

everyone a reminder. You know, DNS abuse is obviously a priority for the Board as a context and a task. We pay a great deal of attention to it, and so we're pleased with the community doing its part to move work forward in this space and really interested in SSAC's role and what it sees as its role in this space too.

RAM MOHAN Thank you. Great question. For the first time in a long time, we're going to be directly involved. We have two seats in the-- we've been invited into that chartering process and into the work that is happening in the GNSO. So we intend to not only opine on it after the comments, which is what we've done in the past, but this time around we're involved in the design and in the decision-making at the start. So that's kind of a different role for us, but we're excited about it and look forward to contributing.

JAMES GALVIN Thank you. Not seeing any questions or comments, so let's move to the Board question that we had to the SSAC. I think we have a slide with that question up here. Oh, okay, already up there. So I'm not going to read that to you. I know that we're prepared for that, so let me just turn that over to Ram for your answer.

RAM MOHAN Thank you. And we did a little bit of work on that, so I'm going to swing to a few SSAC members to provide their high-level perspectives. On the strategic plan, really we wanted to comment

on two things. One is strategic objective 2, enhanced organizational excellence. And in that area, I think the summary of it is that we believe that ICANN should start to focus organizationally, start to focus on performance-based outcomes. And there's generally a focus on making sure there's procedural correctness. This is an important thing, but we would like to suggest an addition of performance-based outcomes. The second part is on strategic objective four, which is the strengthening of the stability and security of the Internet's unique identifier systems, and I'll pass the microphone to Suzanne for that.

SUZANNE WOOLF Thanks, Ram. So I'll talk real briefly, because I see we're short on time, about how strategic objective 4 we're implementing and in some particular efforts, and actually I think this is part of the answer to Jim's question about how do we operationalize what we're doing besides in putting out advisories.

This objective is near and dear to our hearts because it's SSAC's core mission. It's what we're really here for. Current comments, I'll focus on strategy 4.2.1, continue to participate in community-driven efforts to evolve governance of the root server system, such as the RSS Governance Working Group. We've been participating from the beginning, and the most recent effort is the document we published as SAC131. As the SAC comments on GWG outputs, which was a public comment proceeding. This is one of the things we're doing more of is replying to public comment requests. We're

happy to commend the GWG for their foundational work and the RSOs for their stewardship of the RSS. One of the challenges for the GWG is to make a good thing better. We supported the proposed functional model as a good structural foundation.

Our primary message, though, from SAC131, to a great extent, the work to date of the GWG is not even necessarily the end of the beginning. The model still needs further specificity before it's operational. We're urging the new RSS council to prioritize the critical questions that are in the document as having been deferred for further development of the governance mechanisms.

We think the priority is for definition, governance principles, so there are clear guardrails for decision-making, implementation roadmap. There is one in the GWG document, but it needs fleshing out as a structured and staged plan for operationalizing the model. There are some basic operational details, such as the formation of a secretariat and the ability to establish sustainable funding.

Also, there are other bodies in the ICANN ecosystem that the GWG, the proposed RSS council will have to define its relationships with these other components of the community. To tie into the objective here, the continued RSS governance work is a really good opportunity to apply the principles from objective 2. We need to see a commitment to effectiveness, efficiency, and performance accountability in order to make sure that where we are now moves from a concept model to operational reality and proceeds all the way to being complete.

We did note that the comments we offered were very consistent with what various other groups that took part in the public comment proceeding. There was a lot of consistency across the comments, which was, I think, a good sign for our internal process. And we are actively engaged in that process wherever it goes next. So, I think, next up.

RAM MOHAN

Thanks, Suzanne. Appreciate it. Please look at SAC131 for further details in this area. Given that we are a little short of time, I'm going to summarize some of our comments on the other two topics that you have there. We support what the Board is doing with its focus on WSIS+20 review, and we commend the Board in its focus on making sure that the technical community not just has a voice, but a seat at the table. That's an important thing. We strongly endorse that. And we really want to make sure that you understand you have the Org as part of the technical community. You have strong support from us in where you're driving this. Please be and stay in a leadership role in this area. This is important, and we depend upon you to drive that forward.

And finally, on the review of reviews, which has been an interesting topic. We have two members from the SAC who are part of it, Robert Guerra and Suzanne Appointed. And we're also fortunate that you have appointed Jim from the Board to be on that. So we feel like we have sufficient representation there. And what we just want to make sure is you have set aggressive timelines. So please

make sure that you resource it appropriately to meet those timelines. And that's an important thing. This is about ensuring accountability.

So we're really glad that the review of reviews has published timelines. Now your job is to help make sure that they can keep to those timelines as best as they can, given all the various community constraints. But again, we think it's a good step forward. Back to you, Jim.

JAMES GALVIN Okay. Thank you. In the form of a quick wrap up here, I do want to make a couple of comments out of the chat room that I think are relevant here, going back to some prior conversations. A reminder in the question about some of the post-quantum algorithm work SAC has done, SAC107, which talks a bit about quantum work that we're aware of and things that we've done, quantum cryptography in particular.

We also have SAC121, which was an SSAC briefing on routing security, since it was an ask about the numbers community, didn't want to lose track of that. And there was one other one here, OCTO 29 was called out for us for the DNSSEC operational considerations work party. OCTO has published its own step-by-step guidelines and didn't want that to get missed in the work party. I think with that, I will say thank you and turn it over to Ram for a closing comment.

RAM MOHAN Thank you so much. Appreciate this session with you. We always value the time that we have with the Board. I wanted to take just a moment and acknowledge our appreciation for three of your Board members who have served you valiantly and well for their terms and are departing. Becky is here. So thank you for your work. Chris Chapman.

JAMES GALVIN Chris is in the APAC Space meeting, so he couldn't be here.

RAM MOHAN But we wanted to recognize Chris as well. And my friend Maarten, who is there on the floor. But we wanted to commend your work and also commend your continued attention to security and stability matters. You've been friends of this area and we note that. Appreciate it. Thank you so much. Tripti.

TRIPTI SINHA Thank you very much, Ram and Jim, and to everyone around the table for this discussion. Very good exchange of ideas and conversation. And we look forward to the next meeting and updates on the ongoing work. Thank you.

JAMES GALVIN We are adjourned.

[END OF TRANSCRIPTION]