ICANN82 | CF – SSAC Informational Session
Tuesday, March 11, 2025 – 09:00 to 10:00 PST

KATHY SCHNITT: Thank you. Hello and welcome to the SSAC Informational Session. My name is Kathy and I'm the participation manager for this session. Please note that this session is being recorded and it is governed by the ICANN Expected Standards of Behavior and The ICANN Community Anti-Harassment Policy. If you would like to speak during the 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 and speak at a reasonable pace. I will now hand the floor over to SSAC Vice Chair Tara Whalen.

TARA WHALEN: Thank you, Kathy. Good morning. Welcome to the Security and Stability Advisory Committee, also known as SSAC, information session at ICANN82. So, I am Tara Whalen, SSAC Vice Chair, and I'm very pleased to talk to everyone here in the room and all the people we have online this morning and present you with updates on our activities. Next slide, please. So, our agenda for the next hour is, first I will present a brief overview of the SSAC, who we are, what

we do, mostly for those who might not be familiar with our committee and the types of work that we do.

Next, we'll present some of our plans for the upcoming year. Then we'll have some presentations from some of our current Work Party chairs, providing some updates on our paper on DNS blocking and our investigation into free and Open-Source software in the DNS. And we're also going to hear from a future chair for a soon to launch Work Party on integrating new technologies such as blockchain into the existing DNS. And then we'll end with a recap. So, let's dive in. Next slide, please.

So, I will note, for the purposes of the slide, so our SSAC Chair, Ram Mohan, had to present about the SSAC in another session at exactly this same time. So, you're getting Ram's understudy today. So, I'll do my best to channel him and present as well as he would have done. Next slide, please.

So, for people who are familiar with ICANN's mission, part of the mission is to ensure the stable and secure operation of the Internet's unique identifier system. So, this is one of the major responsibilities. And inside of that, as you can see illustrated in the diagram, you have the Security and Stability Advisory Committee. So, this provides expert counsel on matters that impact the security and stability of the Internet's domain name and addressing systems. So, it's an advisory body to the ICANN community and the ICANN Board.

So, you can see we have several responsibilities. So, what we often are doing is conducting a rigorous analysis of potential threats,

assessing operational vulnerabilities, and then deliver some recommendations for mitigating these risks. And as well as recommendations, sometimes we're providing Deep Dive documents. So, we may be helping explain emerging technologies and the effects that these may have on the security and stability of the DNS. Now, because DNS and related systems have a lot of moving parts, we often need to coordinate with other entities.

So, some of these are inside ICANN, like RSSAC for the root server system, but some of them are outside, like the IETF. And collectively, we're trying to keep our security advice and direction aligned as much as possible. And of course, we will connect with the Board and the community, informing them about our recommendations. Next slide.

So, something that we've started to do in the SSAC is take a focus on some particular core topics and try to become a sort of go-to resource on these what we're calling keystone topics. So, there are several security, stability, and resiliency issues within the ICANN community that are core, they're important, they recur, and they're deserving of our attention at all times, pretty much. They're definitely timely, and we get a lot of attention from other groups who want to have our expertise in these issues.

So, we've decided to make this a focus of our work. So, we have an extensive library of work. Of course, the SSAC has been around for some time, and so we have many documents that have been developed over decades at this point. And so, we'd like to use the information that we've collectively brought together over this time,

we want to be actively engaging with the community on these crucial topics. And so, there are two parallel tracks in this initiative. One is around curation and communication.

So, that's really about taking the existing SSAC advice and making it more accessible and digestible. So, it's both making it easy to find and making it easy to understand for a particular target audience. And we're also trying to focus on actionable recommendations. So, wherever possible, we'd like to be able to advocate for concrete steps, particular things that can be done to sort of concretely move forward the security and stability of the internet. And so, you can see the five keystone topics are listed on the slide, and you can expect to hear many of these themes reflected in the Work Party presentations that we'll have later in this session. So, the first of these is DNS Abuse.

This has been a focus area of the SSAC, I'd say almost the beginning really of the SSAC. So, looking at security threats like phishing, malware distribution. Now, of course, last year we had the DNS Abuse amendments to the ICANN registrar and registry contracts that went into effect. Recently, we gave some presentations, for example, at ICANN81 about the use of AI in DNS Abuse. So, this is an area that continues to evolve. So, we're continually studying the area, coming up with recommendations or observations to improve the integrity of the DNS by trying to lower abuse and foster a more secure online environment.

We're also looking at New gTLDs. Well, there have been New gTLDs for, I would say again, probably about as long as SSAC has been

around, somewhere around 2001, something like that. And now we're coming up on a new round. And ahead of the Next Round, there are many issues coming up. So, for example, there were those that were studied in the name collision analysis project, so NCAP, which was a substantial multi-year effort addressing the risk management of security issues that are coming up with the expansion of the namespace.

There's also, of course, DNSSEC. So, we spend a lot of time looking at the DNS security extensions. Though this is a technology that is relied on for maintaining the integrity of DNS information. So, this is a major focus. So, in fact, you've probably noted at all of the meetings, there's usually a DNSSEC or DNSSEC and security workshop that has been put together with the efforts of several SSAC members. That's been going on for many years now. And I believe Wednesday, there's one of these going on here, if that's of interest to you. And these are open sessions. If you want to learn more about DNSSEC, then we're happy to give people information about this.

Another one of the topics is alternative namespaces. So, this topic probably came to people's minds when a lot of the blockchain discussions were spinning up. People were talking about deploying additional namespaces for things like cryptocurrency wallets. But, of course, this is not the first time that these alternative namespaces have come up in this space for systems that are not based on the DNS. The general discussion that arises is what does this mean for the DNS? So, how do these systems

coexist? And so, I mentioned earlier, so we're going to have a teaser later this session on a new Work Party that's focused on this area.

And finally, there's Internet Governance. So, something as globally significant as the internet is accompanied by serious governance issues, including security and stability issues. So, there are major technological policy aspects there. So, in our role as technologists, we want to be able to provide good advice for policymakers. People are making decisions on many of these technical policy issues, and we'd like them to be grounded in good technical advice. So, they may not understand, for example, how the DNS works, which could lead to some misguided solutions.

It's understandable, but we try our best to help them to make better decisions. Finding ways to ensure that our advice is pitched in a way that could be accessible to someone who is trying to reason about it while they're making some kind of a policy decision. So, we're trying to tell them what are the crucial security, stability, and resiliency topics, and also to make them aware of the implications of certain choices. So, often people have to think about not only the thing they're intending, the intended effect, but there may be some unintended side effects of the regulation that they need to keep in mind. Next slide, please.

So, here's a snapshot of the whole SSAC. I guess there's 38 of us at this point. Here's our happy faces. We have technical experts from all around the world. We have a lot of new members, so we're delighted to have new faces helping to contribute to SSAC's work. Right now, we're still a bit concentrated in North America and

Europe, but it's gotten better recently. We're delighted to have people from a few new regions in our membership, and we're hoping to do even more. We definitely like to, for example, look to see if we can get more representation from Latin America, from the Caribbean, and I'll return to that when we talk a little bit later about membership.

I'll also introduce you to the leadership team for the SSAC, sort of basically the steering committee. Ram and I have formal roles as chair and vice chair, and as does Jim Galvin, who is our Board liaison. We also have two other members who've stepped up to take on significant responsibilities, who are seated next to me here, Jeff and Barry. And so, I think we found this to be extremely helpful for balancing our workloads, leveraging our different skill sets, and just having more hands-on deck when we're trying to move initiatives forward. You know, helpful, for example, when someone is called away to a parallel session to give a presentation, and one of us can step in when the chair isn't there. And fundamentally, we just work really in a collaborative, fundamentally collaborative way.

And of course, so far, I've only given you half of the slide. We also believe that our ICANN policy support staff are an essential part of our work, who you will see also on our slide. So, we wouldn't be successful without the policy support staff's effort. So, they have expertise that's really vital for us to accomplish our goals. So, this could be things from policy training, so they can help us shape a message for a specific audience, or they may have writing skills to bring clarity to our technical content, or have research skills that

identify a useful resource, as well as fundamental project management skills, or they have deep connections as well in the ICANN community.

So, that's key for our having successful collaboration with other groups. And overall, ensuring the advice that we put out is technically sound and directly relevant to what ICANN and the community needs. All right. That's the end of the overview of SSAC and its members. So, we'll move on to the next slide, which involves the plans for 2025. So, I'm going to give some highlights of some things that we have in mind for the next year. So, of course, we are going to have some Work Party updates, which is a major part of 2025. But first, I will talk about our strategic goals.

So, the SSAC has set six strategic goals for a three-year period. We're now in 2025, in the middle of it, for enhancing its impact and efficiency within the ICANN community. So, these really reflect our commitment to security, stability, and also member engagement. And the leadership team has worked on a set of objectives and then changed practices for each of these goals to bring them into being. And so, I'll note of the overview here, goals one, three, and four are a little more focused on the content, the SSAC advice. So, making that relevant, getting it distributed efficiently, and concentrating on those keystone topics that I mentioned earlier.

And two, five, and six are focused on the members. So, connecting people with tasks that make best use of their skills and interests, and recognizing the valuable work that our members do, and improving our membership diversity. Next slide, please. So, one

half of those goals can be categorized as the community-facing plans. And what we did as the leadership team is that we spent multiple days, actually, in 2024, mapping out detailed plans to advance each of the goals. We had concrete steps and associated timelines. And so, this is a snapshot of that content, highlighting the major items for 2025.

So, the community-facing plans, so here are the first one about enhancing the quality and relevance of our advice. So, you can see some of the work that's expected to be delivered in 2025. There are the two current work parties, the DNS blocking and the free and Open-Source software in the DNS, which you'll get updates about. We also have two new work parties in the pipeline. So, the first of these, the responsible integration of new technologies in the DNS, you will hear about that shortly. But we're also looking at DNSSEC assessment. So, that is investigating the current state and operational realities of DNSSEC and alternative security technologies and barriers to adoption.

So, the first one, what we're calling RIDE, is about to start. The DNSSEC assessment likely won't start until one of our current parties completes. We don't want to overstretch ourselves. And I also note for this, in terms of our advice, we are trying in the SSAC to be quite deliberate about the outreach that we do. We want to ensure that we're providing advice that the community needs. So, we've been having more conversations with the various SOs and ACs, both to get a better idea about the types of questions they have. So, that's, well, what are we going to need to prioritize based on what we're hearing from the community? And also finding how

we might better get our advice out to these audiences in a useful way, which ties into the next item about strengthening our voice on crucial topics.

So we've been working with the ICANN staff on communication strategies because we don't only want the recommendations to be available just in the detailed SSAC reports. And we figure that there are probably more ways that this advice can get out to a broader community. So, we've had lots of conversations. For example, we were talking with ALAC about the Safer Cyber Education Campaign, which was advice for non-experts. We now are starting to have 500-word summaries, thanks to some of our energetic new members who went back and looked at some of the publications on the Keystone topics in order to make some of the content more digestible so people can get a snapshot and decide if they want to read a little bit more.

And also, our members are often active in professional communities and various events like security conferences. And so, we'd like to leverage those opportunities as one way we could maybe spread the word about our publications as well. And the third of these is enhancing diversity. So, we think that 2024 was a pretty good year for membership. And of course, I'm not just saying that as the membership committee chair, but we had a lot more applicants than we'd had in the previous years. And we had nine new members. And we'd like to build on that.

So, we want to ensure that our new members are integrated well, onboarded well, and can start contributing early and have

interesting work and can thrive as an SSAC member. And I'll note, we started having more open meetings last year. That's a departure from a tradition of mostly closed meetings. And I think this helped us reach a different set of applicants than we'd had previously. We do acknowledge there's a gap in Latin America and the Caribbean. So, we're doing targeted outreach here. So, I've had some suggestions from people about different individuals and groups to connect with to improve our coverage here, which has been great. And I'm also happy to learn about more. And by the way, the membership application window is currently open. So, please do reach out and talk to any of us, particularly me. Next slide, please.

So, for the other three topics are more internal facing about how we might improve our own work, such as how our members are doing and how is their engagement, how are our work process working, how is people's expertise working to connect it to the broader community. So, the first of these is about boosting engagement. So, we want to ensure that the SSAC members are actively contributing. And to that end, we do have some plans for the next year.

So, we want to have a, for example, a better definition of active membership, sort of what it means to be engaged with examples of ways in which people can contribute. We think this is particularly helpful for new members who may not know, for example, of relevant opportunities for their skills and interests and to figure out what the general expectations are. And we're also continuing to work with tools, like we spun up an informal slack for strengthening

real-time collaboration. And we've designed our meetings to be more interactive. So, instead of being sort of status reports, a lot more discussion times for us to interact with each other.

We're also looking about trying to get our work products out efficiently. Things move fast. So, we'd like to be sure that when we get a report finished, that it's still relevant to the world in which it was. Hopefully the advice is still relevant to the situation for which it was developed. So, some concrete actions we have planned here are, for example, a chair skills guide. So, because the chair is key to the success of any Work Party, we want to give them all the help that they can get.

So, we're drafting a guide. And in support of this, we're holding a session this week with a panel with some of our experienced chairs to have a discussion, to talk about challenges and ways of getting past obstacles. And I'm looking forward to that later today. We're also planning to define more clearly the various roles of Work Party members. So, expectations are clearer. You can have different roles. You can be not just a chair, but you could be a contributor. We have staff who are contributing to the work parties as well and reviewers. We want to be sure expectations are clear and so that their collaboration works more smoothly overall. And of course, it's important to assess whether these goals that the leadership team originally made are working as intended. So, we plan to have an annual review and then update the strategy accordingly, refine and iterate. And as we move forward to that, we're pointed in the right direction.

The last of these is about supporting expansion of expertise. So, we want to make sure that our expert volunteers are getting the recognition they deserve. And they do a lot of hard work. I think it can sometimes seem like a thankless task. It's slow moving, difficult work, coming with consensus on complex subjects. So, we want to raise the visibility inside SSAC and in the wider community. Additionally, we'd like to know whether members have areas that they'd like to delve into more. They maybe want to broaden their knowledge base.

So, for example, there might be a different area within ICANN they want to learn more about. And if so, if we can find an opportunity to take advantage of that, because none of us knows everything, but collectively we can cover a lot more ground.

Next slide, please. So, of course you can ask questions during the session, but also, I will note that we have an open mic on Wednesday in block two. So, we are friendly people. We would love to hear from you. So, come to the open mic session. You can ask us about the current work parties. You can ask us about any of the reports or the recommendations that we've made. If you want to ask about SSAC membership, you're more than welcome to, or any other SSAC related topic, please come. We are absolutely delighted to hear from folks during that session. Or you can also grab any of us if you see us on the coffee breaks, but this is dedicated for you. All right. So, that's it for this section of the presentation. So, I'm going to stop now, check the queue, take any questions before we move to the next part.

ROLLA HAMZA

Good morning, everyone. This is Rolla Hamza for the record, ICANN fellow, and I'm speaking by my own capacity. I wonder if there is, you highlighted that there is a working group on blockchain. I wonder if there is, instead of focusing in blockchain only, there is an emerging technology that quantum computing AI that impact the DNS, especially that the new technologies is focusing on one technology will not be sufficient. And there is a new technology that needs to be on focus. Thank you.

TARA WHALEN

So, that particular Work Party, we have tried to be careful in the scope that we have for a particular Work Party, because it has to deliver a document that's focused enough that we can complete within a reasonable time. But we are tracking a lot of emerging technologies. I'm looking around the, when I look around the table, I can see that we had a presentation just recently about the effects about post-quantum. I'm looking now at the end at Russ. I know that we had Jeff giving a presentation conjunction with Lauren about AI and DNS Abuse.

So, you will often find that we have threads of these in some of our other reports. But you are correct in that we don't want to try to just focus on one thing because there are always new emerging technologies and new threats. But then the trick is figuring out how we fit that into the way we do the work product. And then sometimes instead of it being a report, it may be something like one of these presentations that we give where we can highlight

some of these threats, particularly talk about them in front of one of an audience like this to make them aware of those things.

MOHIBUL MAHMUD: Hi, it's Mohibul Mahmud for the record and I'm an ICANN fellow. So, I have a question like how SSAC collaborate with other organizations like IETF and RIRs to ensure a secure DNS infrastructure?

BARRY LEIBA: There are, well I'll say that many SSAC members participate in the IETF and in other organizations. So, what?

TARA WHALEN: Yes, many of us do.

BARRY LEIBA: Many of us do. So, that's the question. There's a lot of just sort of cross-community work that's being done. We also have joint meetings with various other parts of the ICANN community like ALAC and that sort of thing. So, we don't specifically target like the RIRs, but we are in conversations with them and they read our documents and we do have input back and forth. So, that's the main focus. One of the things we strive for is a broad variety of skills and a broad variety of communities that we have tendrils into when we're looking for new members. We're looking for diversity of backgrounds and diversity of participation and skill sets. Tara?

NABIL BENAMAR

May I add just something here? So, I'd like just to add that, maybe based on my modest experience that SSAC is maybe the closest group to the IETF work. So, there are a lot of similarities between SSAC and you can see that major members of SSAC are active members in the IETF and they have already published several RFCs.

Maybe in SSAC we are not publishing RFCs, but the need for any new technology or RFC or standard may be born here before it's been taken to the IETF. So, if you are really interested in joining because you are a fellow, if you are looking for this, for example, participating in the IETF would be an added value for you, for your CV, for your profile. Thank you.

BARRY LEIBA

And this is Barry Leiba. I want to highlight two SSAC sessions today that I'd like everybody to come to. We have some lightning talk sessions, which to me is one of the highlights of the week in SSAC. We have SSAC members and people that SSAC members connect with who come and give 20-minute talks on interesting topics. And we have one next session next door at 10:30 and then one at three back in here. So, please come to those. I think you'll find them interesting.

TARA WHALEN

Thank you, Barry. All right, with that, I think now we will jump into-

RUSS HOUSLEY It's probably worth saying that those lightning talks are a little on the technical side.

BARRY LEIBA Yes, they tend to be technical topics. I think Liao is going to do, she says she's going to do a lighthearted one. So, that should be interesting.

TARA WHALEN All right, that's good advertising for the later session. I like it. All right, so now I think we are ready to jump into the first Work Party update. So, over to you, Greg.

GREG AARON Thank you, Tara. My name is Greg Aaron. I'm the co-chair of this working party. The other co-chair is Warren Kumari, who's at an IETF meeting today in another part of the world.

And so, if we can go to the next slide. Let me tell you a little bit about what this project is. The working party has got its draft together. We've been working on it about six months. And now we're going to go through a review process where the whole SSAC reviews it. It'll make some updates. But our goal is to have this paper published in the spring in advance of the next ICANN meeting, which will occur in June, at which point we will present the project fully and tell you about the exact content of it.

So, we encourage you to come back in June to hear all the details. But we want to update you today about what this is. So, what's DNS blocking and why is it important? When you want to go to an

internet destination, for example, you type something into your browser, you type in a domain name, it's translated to an IP address. Basically, the DNS is helping figure out where your query is going to go and how you're going to reach the destination and the content you want. And usually that works fine. The translation works, you get to the place where you want to go. DNS blocking is a practice or technique that interferes with that process.

So, it's a fundamental manipulation of the DNS. And it's done in different ways, which we will describe in the paper. But one thing you can do is send somebody to an alternate destination. Or you can say that a domain doesn't exist when it actually does exist. Or you can not send back a response at all. So, DNS blocking is a way of preventing somebody from getting to a location or reaching some content.

Now, this is a technique, it is a tool, it is a practice. And like all kinds of tools and practices, sometimes it can be used for things that are useful. Sometimes it can be used clumsily. Maybe sometimes it's not the right tool to use for your goals. DNS blocking is used for a lot of different reasons and a lot of different motivations or social motivations. We're going to talk about the technology. We're going to give case studies in the paper about how people have done things for various purposes. And we're going to talk about the implications. Because sometimes if it's not done well, or it's not the right technique, there are a lot of implications and side effects and unintended consequences.

So, if you can go to the next slide. So, one of the most controversial things about DNS blocking is sometimes it's ordered, say, by a court. Sometimes it's accomplished at the order of a government. One of the ways that it is used is in service of censorship, which is probably the most controversial thing. So, one of the audiences for this paper is policy makers and people in government. Basically, our approach is, it's important for everybody to understand how this works and how it might not work so well in some circumstances.

That's useful for everybody to know how these things happen as a user, as someone who's considering doing it. As technologists, we're not trying to make judgments about some of the particular cases or implementations. That's more of a sometimes a political or social discussion. So, this is basically an educational paper. We will probably not have any recommendations to the ICANN Board, for example, as we sometimes do in our papers. So, we hope it's a paper that will teach people about how this works, why it's important, what you need to know.

And the next slide. And basically, I just said all that stuff. So, anyway, we want to get it out with enough time for the community to read it and digest it. And then in June, we'll have some fuller presentations about it. And that's going to be a real opportunity to dig into questions and so forth. So, we're giving you a heads up now, hoping to generate some interest. And we can take any questions that you have in the meantime, though.

MOHIBUL MAHMUD: Hi, it's Mohibul Mahmud for The Record. And I have a question to Greg. First of all, thanks for the insightful presentation. And my question is, how can we block harmful websites like using DNS without accidental blocking good websites? And like, what SSAC recommendation for that?

GREG AARON: So, the paper will talk about how DNS blocking can be done at various levels, so to speak. For example, it can be done just within a corporate network, for example, or a university network, for example. That's done quite commonly. It can be done at ISPs and so forth. One of the things that paper is going to talk about is who do you have control over? Who is your set of users? What is your realm of responsibility if you're going to be considering blocking?

We will have a section that talks about the use of DNS blocking for security. It's actually quite common. And actually, most of us are protected in one way or another by DNS blocking techniques. Some of the associated issues are how do you choose what to block? Are you letting people know that the blocking is occurring? Who are you affecting? Are you affecting people outside your realm of responsibility and so forth? So, those kinds of topics will be covered in the paper.

NABIL BENAMAR: Yeah, so can't we think or see that DNS blocking can be considered as an attack itself since it's a denial of service. You are blocking me to access something or somewhere. So, this is an attack. So, it has

been done previously in the ITF when they published the RFC 7258, which is pervasive monitoring is an attack itself. It was considered as an attack. And from that time, they have started thinking seriously on the encryption and all stuff. What about DNS blocking? Thank you.

GREG AARON

This is very much situationally evaluated. All DNS blocking is definitely not an attack from our viewpoint. So, the paper is going to talk about whether there's knowledge of it, consent, at what level it's happening is very important. The more people you're affecting or are responsible for, the more of these questions become important. I don't think that RFC may deal with certain situations, but it does not deal with all uses of DNS blocking. Barry.

BARRY LEIBA

Yeah, this is Barry Leiba. Let me expand on that a little bit. The intent of the IETF RFC is to say that pervasive monitoring is indistinguishable from an attack. If you can't distinguish a government monitoring you or a parental monitoring or something like that from a bad actor monitoring you. For blocking, there's a little bit of a difference. We certainly accept blocking broadly for CSAM material, for instance.

Parents can intentionally sign up for a blocking service to protect their children in the household, things like that. So, it is, as Greg says, more nuanced. And that's what we're trying to tease out in

the paper, not in detail, but pointing out the different situations that can occur.

TARA WHALEN

All right, that's all of the questions. Thank you, Greg, for your presentation. Now we'll move on to our next one. So, the floor is yours, Maarten.

MAARTEN AERTSEN

Good morning, everyone. So, my name is Maarten Aertsen. I'm a member of SSAC, and I have the pleasure of chairing a Work Party on the use of free and Open-Source software in DNS and domain name registration infrastructure, which is more text and fits on this slide. I am not doing this alone. My co-chair is Barry Leiba, who you've just heard speak. And there's a bunch of us slowly progressing towards a paper that we hope to publish in June.

So, for those that don't know, free and Open-Source software is software that has a license that allows you to use, study, share, and modify software freely as compared to software that does not have these properties. So, this paper will look into the situation where global infrastructure for DNS and domain name registration heavily relies on Open-Source software.

This is, among practitioners, a reasonably well-known and established fact, but it's not being, like there was no previous work documenting this. And this is problematic when policy is being developed or policy discussions are being had about software systems generally and infrastructure generally, where this state of

the world is not being considered. So, this Work Party is trying to document the fact that there are certain rates of deployment to the extent we have data to back this claim.

And then to explain that this free and Open-Source software has a relatively unique development and governance characteristics as compared to most other goods in markets beyond the digital sphere. And if you are regulating a software or infrastructure space, it makes sense to be aware of these economics. So, like the DNS blocking paper, this is mostly an educational effort where we will not be offering recommendations to the ICANN Board. Instead, the idea is to clear up misunderstandings about free and Open-Source software that can lead to policies or regulations that inadvertently weaken global infrastructure.

So, it's basically two parts. We try to make a landscape description, this visibility, and then we hope to provide educational material to help policymakers reach their policy goals, which is what they want, without unintentionally harming an ecosystem that can have security and stability implications in DNS, which is what we are chartered to do and kind of fits these teams together as I work.

So, a little bit like the DNS filtering paper, we try to write for a policymaker audience. We do not interact directly with policymakers unless they are already part of the ICANN community, but instead we try to make a work product that is useful for the internet community at large in their conversations with legislators and regulators. So, the idea would be to make like referenceable material that is available when such conversations

are had. And as an example, myself in my personal capacity outside of ICANN, I've had such conversations and I was missing this reference material.

So, this is kind of how we have a bit of a new type of product here where the writing may not actually be directed to the technical community as much. Instead, we try to make a paper that is readable in a policy sphere. Which has its own, I guess, challenges because that's not what we've been doing as much in the years of publishing previously. So, if you're in the audience today and you learn more about this work over the next few months, be sure to give us feedback whether what we made was actually readable if you are in the policy sphere yourself.

So, the paper will address four areas. Like I said, it starts with a description of the landscape. So, we try to map the use of Open-Source software across a number of infrastructure areas. Most prominently, authoritative name servers which is the component where DNS answers are given. Recursive resolvers, which is basically the question side of DNS where questions are asked. And the domain name registration component where domains are registered, they are administrated. And by that functionality, the ability to publish in the DNS is delegated from the top level. So, we make a landscape description. What's the world like right now?

And the second part of this paper is to describe the characteristics of Open-Source software. We zoom in from like a general description towards the characteristics that are most, like that occur with development of popular DNS systems. So, it's not about

Open-Source generally, it's about Open-Source as it is consumed in like our sphere in a sense. The third part of the paper is about the operational side. So, what makes operators consider Open-Source software as their chosen solution? Because they have full freedom to choose and if they choose for Open-Source software, they have reasons to do so.

So, this tries to analyze what characteristics influence this evaluation. And because we're SSAC, for both the green and red pie, so the right hand of this diagram, we specifically look at security and stability considerations. So, it's not just a general description, we look at the security side as well. And then the final part, which is probably where we provide most value in the policy sphere, is we give specific examples of misconceptions which are common, they are quite logical to arrive at, but they're also misconceptions because they don't carry, like the logic doesn't carry on to the use of Open-Source software.

So, I'll give an example, one that we heard a lot when we did a workshop in Istanbul to get input for the community, is that people are confronted with the statement as fact that Open-Source is less secure generally. And this may be true in specific instances, maybe it's true in very many instances, but it's not something that you can conclude from the license, it's basically a perpendicular consideration. The other misconception that I'll name that is not on the slide right now is that in the physical world, if you build complex infrastructure, the entity building this infrastructure needs to be powerful in some way due to inherent material cost.

So, for example, if you need to build a bridge, a bridge has materials, materials have costs, and so the actors building bridges tend to be financially very sophisticated, and with that sophistication in financial sense comes economic power. In contrast, in the false world, it can be very small entities that make the software that everyone uses, so this conception that complexity equals cost power does not always hold. And this is relevant, both the fact if you are making law, because you might assume that certain assumptions hold and certain types of policies will be effective.

So, these are the four key areas of investigation. We are aiming towards publication in the summer, and you'll be able to read a more nuanced version of everything I just said in our report. Thank you for your attention, and I'll pass back to Tara unless there's any questions.

TARA WHALEN There aren't, thank you, Maarten. We can start with the questions.

MOHIBUL MAHMUD Hi, it's Mohibul Mahmud for the record. My question is like DNS is actually, first of all, thanks for your nice presentation, and DNS relies mostly on the free and Open-Source software. So, what is your observation, like how could we stay, keep staying secure and reliable this Open-Source software? Like what is your observation? How could we make it, yeah?

MAARTEN AERTSEN

So, at present, I don't think SSAC has a position on answering this question, but we're working towards it, right? So, when we publish a report, maybe this is one of the aspects that we address. I can give a personal answer, though. I think personally that the security of software is mostly independent of its chosen license. So, if you have software which has a group of maintainers that actively works towards securing it, you have a much higher chance of having secure software.

So, it's more of a property of the group of developers, the funding they receive, the input they receive, than it's necessarily a property of the license. But in an area of DNS, what ends up happening is that there is a pretty active academic research community looking at the security of the protocol and of the software. There has historically been a number of players that are in there for the long game, and in some case, non-profit entities. And I think these are characteristics that play into the question that you ask, so.

DANIELLE RUTHERFORD

Thank you. Okay, Barry, and then we have a question from Abdul Karim.

BARRY LEIBA

Hi, yeah, this is Barry Leiba. One of the things that we're trying to tease out in the paper are the differences between open-source and proprietary software in the aspect of maintenance, particularly with security vulnerabilities. So, like, for instance, on the one hand,

if you find a security vulnerability in open-source software, you can fix it, or you can get a team that works with you to fix it. On the other hand, on proprietary software, there's somebody who's signed up and being paid to get that fixed. So, there's a balance. And again, as Maarten said, people make decisions to use one or to use the other, and that's part of their decision process. So, we'll be talking about that in the paper.

DANIELLE RUTHERFORD Thank you, we've got Abdulkarim, and then I think Nabil in the queue, and then we're going to have to cut it there to get through our last presentation.

ABDULKARIM OLOYEDE Okay, thank you very much. You mentioned publishing a paper. I would like to seek some clarification on what kind of publication you mean. For somebody like me coming from the academia, publishing typically refers to publishing in a recognized journal or a conference. And since you mentioned that the goal is to have a paper that serves as a reference, so I would like to know if the plan is to submit it to a journal or a conference.

And also, does RSSAC have a specific journal or conference where they publish their paper? Then quickly, my second question is, you talked about the intended audience. The key areas in which you describe seems relevant to both newcomers and technical experts. So, how do you plan to structure the publication so that both

groups can benefit? And also, do you plan to have a single paper or is it going to be multiple papers? Thank you.

MAARTEN AERTSEN: Thank you, Abdulkarim. So, towards your first question, the citability or referenceability is mostly towards policy work by the internet community. So, we're not targeting academic publication. And your second question.

BARRY LEIBA: Yeah, let me expand on the first question. In general, SSAC publishes our results on the SSAC documents page on the ICANN website. They're not formal publications to any journal or conference. Yet they can be cited. I mean, it's not academic work, but it can be cited.

MAARTEN AERTSEN: And I think that was the second question that was mentioned. So, I saw a hand from Nabil, but I also saw a hand from someone who's not an SSAC member. And if Nabil is okay, I would like to give the other gentleman a chance to speak.

VINNY ADJIBI: Thank you very much. Appreciate that. My name is Vinny Adjibi. I'm an SSAC participant. My question is related to, so you talked about free and Open-Source software being used a lot in DNS and how regulation can affect the use of those software in the operation of the contracted parties. And one thing is that Open-Source

software comes in different shapes. So, we have various licenses. The type of license under which the software is distributed might affect the way in which regulation affects it. So, are you going to be looking into how GPL or other type of licenses affects regulation or so on and so forth?

MAARTEN AERTSEN: So, I think we would not be the best entity to dive into the specific of these copyright licenses. Where there is a specific difference that affects the scope of our paper, we might look into this. And thanks for suggesting it. But at this moment, I think we stay at a very high level and then reference one or more sources that are way more authoritative on this side of things. Because we are not a group of legal scholars in that sense. Thank you for the question. And I'll pass back to Danielle. Sorry, to Tara. Apologies.

TARA WHALEN: No, thank you, Maarten. So, we have one more presentation. There's just one more thing. So, we have our Matt Thomas, who is remote, I believe, to talk about an upcoming Work Party.

MATT THOMAS: Thank you. Can you hear me okay?

TARA WHALEN: We can.

MATT THOMAS

Great. My name is Matt Thomas, and I will be co-chairing a new Work Party with Rick Wilhelm. And it is going to be focused on responsible integration into the DNS ecosystem or the RIDE acronym there. The Work Party really hasn't started yet. So, I'll just be giving a brief introduction to RIDE Work Party and what its scope is. So, if we can go to the next slide, please.

So, as emerging technologies like blockchain or decentralized platforms start to integrate with the public global DNS, they need to start accounting for established domain name lifecycle to avoid things like unintended consequences. In the past, SSAC has had studies on things like the public suffix search list, the PSL, and HTTP strict transport security or HSTS, and then examine the impact of those technologies into the DNS security and stability.

More recently, we had a SSAC report 1.2.3 come out, which explored how evolving name resolution models interact with the DNS. And building off of this foundation, the SSAC is now going to launch a new Work Party that looks to assess the risks and requirements for responsible integration with existing and new technologies that align with the DNS ecosystem without compromising or impacting its reliability. Next slide, please.

So, the responsible integration of third-party tech into the DNS clearly requires understanding how those types of technologies interact with the domain name lifecycle and specific events around things like registration, transfers, and renewal. This specific SSAC Work Party is going to examine risks around name collisions, security vulnerabilities, end-user confusion that could arise from

misaligned integrations. So, it's also going to take a look at reviewing whether existing ICANN policies sufficiently address these challenges or if updates are needed.

The goal really of this Work Party is to provide some practical guidance back to the ICANN community in general, as well as the technology developers to ensure that new integrations support the security, stability, and reliability of the global DNS. And with that, I think I can hand it back to you, and we're almost at the end of time.

TARA WHALEN

Thank you so much. Thank you, Matt. I don't know. All right. And then Rick is giving you a thumbs up in the room. So, now we're in our last two minutes. So, if we can move to the next slide and just give a very brief summary. The first thing to summarize is I'm still not Ram Mohan, but on the next slide, we'll give you a snapshot of the work we presented. So, a few highlights. You can be expecting two reports coming out and the launching of two new work parties. We'll be working on our own internal improvement around internal definitions, expectations, member engagement. We have presentations here about DNS blocking. As you'll note, as Greg presented, the landscape evolved and our guidance has had to move along with the changes.

We're also going to be talking about the free and Open-Source software in the DNS as described here, how the DNS sausage is made or the sausage bill of materials or something.

BARRY LEIBA I like how the DNS tofu is made.

TARA WHALEN Sure. The DNS tofu sausage is made. And in the future, about integrating new technologies, how to play nicely with others. And with that, I guess our next slide says questions, but you've been giving excellent questions all along. So, we've integrated them into the presentation. So, I think we're at a good place for us to stop. And I thank you all for your attention and your excellent questions. And you can talk to us throughout the rest of the week. This is not your only time to ask us questions. Thank you very much. Thank you to the presenters.

BARRY LEIBA Thanks, everybody, for coming and don't forget to come to the lightning talks. Thank you.

[END OF TRANSCRIPTION]