ICANN78 | AGM – Joint Session ALAC and SSAC
Sunday, October 22, 2023 – 1:15 to 2:30 HAM

YESMIN SAGLAM: Hello, and welcome to the ICANN joint session of the ALAC and SSAC. I am Yesim Saglam, and I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior.

During this session, questions or comments submitted in chat will only be read aloud if put in the proper form. As I've noted in the chat, I will read questions and comments aloud during the time set by the chair or moderator of this session.

Interpretation for this session will include English, French and Spanish. Click on the Interpretation icon in Zoom and select the language you will listen to during this session.

If you wish to speak, please raise your hand in the Zoom room and once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the Interpretation menu. Please state your name for the record and the language you will speak. If speaking a language other than English when speaking, be sure to mute all other devices and notifications.

Please speak clearly and at a reasonable pace to allow for accurate interpretation.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real time transcription, click on the Closed Caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multi stakeholder model, we ask that you sign into Zoom sessions using your full name; for example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I will hand the floor over to Jonathan Zuck, the Chair of ALAC.

JONATHAN ZUCK: [inaudible] We've got a number of things coming up related to the next round that we talk about jointly, and we have this thing called the At-Large Loop, which is some experiments in trying to really systematize our engagement out through our membership and out to end users and things. And one of the topics that would be interesting that we discussed in our last meeting was DNSSEC, which is why we wanted to make sure that Mr. Crocker was here to figure out what we might do in terms of coming up with sort of end user accessible messaging around it and do some experiments of getting that word out through our network.

So we've got a lot of exciting things to talk about, and welcome, everybody, and thanks for being here. We've got a full house.

Rod?

ROD RASMUSSEN: Thank you, Jonathan. Thank you to the ALAC. This is one of our favorite meetings as well, and Jonathan and I do a bit of rabble rousing whenever the chairs all get together, so we often find ourselves in alignment and maybe not with everybody else. It's all good. It's our pleasure to be here. I'm glad to hear that. The technical items we're about to discuss are exciting. It's good to have an audience enthusiastic about that.

Also, you're mentioning the outreach capabilities. We also talked about last time potentially getting some of our publications out to your network as well. And one of the things we're going to be talking about today are the three publications that are likely to be coming out in the next three to four months and hopefully not all the same day (we won't do that to you) but very soon. And some of the documents we've actually been pre-sharing those a bit about drafts with various folks around the community.

One of the things we're doing in the SSAC is working on our transparency a bit. One thing I wanted to point out to folks is that at this meeting, several of our working sessions are open, which is new. It has not happened before, so that you'll actually see those on the calendar as open sessions. And we're going to move more towards a model of default open. So that is a relatively new development.

We've been trying to do more, as I said, pre- screening, so to speak, of documents, which has helped us make better documents and certainly helped us get better reception for recommendations and such when people have had a chance to think about it before you make the final call on that. So that's something that you guys might want to think

about as well too. I know there has always been some back channeling of some of these things, but being a little bit more purposeful on that I think is useful. So for this meeting, we want to make sure we're updating you on what we're about to come out with and think about ways that we can bring that to the broader ALAC community.

JONATHAN ZUCK: Well, I'm very glad to hear that you're getting over some of your insecurities and more accepting of some instability through these open meetings. So that's real growth.

ROD RASMUSSEN: I'm going to use that one too.

JONATHAN ZUCK: So the first item on the agenda is DNSSEC capacity-building. As we spoke briefly in the last meeting, we're currently working ourselves on how to manage campaigns of either information distribution or feedback. So both of those things. You might hear mention of the At-Large Loop, which is a series of experiments basically in the best ways and what tools we have to get information out to the community or to get information back from them if we're trying to do policy development internally, position development internally, and we want more voices to be part of that process. And so systematizing that is something that's what we're referring to when we talk about the At-Large Loop.

And so we're planning on doing something very similar to UA Day on the issue of phishing, for example, and talking to people about how they can recognize phishing attacks and how they can use some of these new tools that came out of the Contracted Party House (the asset tool, the [beacon] tool, et cetera) to report phishing. And so that might be our first experiment in one of these sort of mobilization activities.

But the last we talked a little bit about DNSSEC, and the challenge, I think, with that particular topic is to come up with a set of messages and explanations that can have broader understandability and sort of deeper into the end user community, if you will, than just our policy team.

And everybody immediately said, well, the master at doing that is Steve Crocker. And so that's why we wanted to make sure that you were here. Part of that meeting is to have a little bit of open conversation about what you think we might be able to set objectives, because what the call to action might be is bringing it up with your employer or something like that and kind of understanding what role users could play in advancing the cause of.

So with that, I guess I might pass it to Steve to ruminate on it a little bit.

STEVE CROCKER: I'm going to make it interesting for you.

JONATHAN ZUCK: Oh, all right.

STEVE CROCKER: So one of the lessons in graduate school is when you're being examined, particularly in an oral exam, if you can't answer the question, substitute the question and answer that always. So I have a different topic that I want to bring up, but I'm not going to ignore DNSSEC, but I'm going to—

JONATHAN ZUCK: [Just say, "]Rod, now the second thing on the agenda is…

STEVE CROCKER: So I'll talk for a minute about DNSSEC and then I'll tell you what the other topic is. You won't be terribly surprised, I suspect. Around 30 years ago, an amazingly long time ago, there was an attack discovered with DNS in, which was a cache poisoning attack—that's what it was called—and somebody could insert into the network an answer to a query and beat the official answer coming back and fool the requester and get them to go to the wrong place. And not only was that organized and documented from a theoretical point of view, but software was built and demonstrated and it was surprisingly and quite alarmingly super effective.

At the time, I was vice president of a small company that focused on network security. And my good friend Vint Cerf, who was well-connected even back then, called me up and said, Steve, we have a problem. And it turned out that this attack had been demonstrated by somebody at the San Diego Supercomputer Center. The director of the San Diego Supercomputer Center was not only a senior person in his own right, but he was plugged into the very highest levels of the US.

Government, connecting to the presidential science advisors. So this thing rocketed around at very high levels and caused issues.

So in rapid order, we formulated a research program to try to add security to the domain name system. And it only took on the order of a decade to work it all out, because it turned out to have some complexity and it turned out to have some differences in points of view and so forth.

So the DNSSEC saga has been going on for a very long time, and with multiple bumps along the way. One of the bumps that was experienced fully within this community was a debate about whether to have the route signed or not signed. The Department of Commerce was hesitant for a few years. All that's way in the past. The root was signed 2010, I think. And so now we've had more than a decade of that's been under control.

So how are we doing? Well, you really have to measure. It was two different things you have to measure and you have to measure the first thing in two different ways. So the first thing is, how much implementation has there been of the DNS security? And the two halves of that are the signing side and the checking of signatures, so-called validation. And on the signing side, ICANN has had a rule for a long time that all of the gTLDs have to be signed and they have to permit registrations of those registrants. And the cc community, which is not bound by ICANN rules, and nonetheless been coming along pretty well. So there's good measurement of what the signing has been at the top level.

How well has that gone on below the top level? Not so good, not zero, and progressing, but a long way from being totally dominant.

On the validating side, the statistics are related but worse; that is, there's less validation than there is signing. So there's a lot of signed answers that are provided for, which we believe there's no checking that has gone on.

So that's the first thing that one can measure and observe. Another question is, well, how much does it matter? Well, there's a more tricky question. There's not been a lot of cases of cache poisoning, I must say. There are a lot of other security issues that have come along, and other forms of abuse.

So while we're pushing very hard (and I'll say a few words about it at the moment, about the campaign to keep going with DNSSEC), we're beginning to hear reasonable, sensible, experienced people saying, when you've been working at it this hard for this long, maybe it's time to stand back and say, okay, where are we going?

The original objective (and I took a fair amount of money from the government to help in this process) was every zone signed, every answer signed, every answer checked, 100% across the board. We're not there, and we may not ever get there.

And then the question is, well, does that mean that it's no longer useful? Or does that mean that there is an intermediate settling point where important things get signed and important things get checked but other things get handled in another way? And there's competing technologies of HTTPS and several others. So you might choose to hear that as a

negative or as a depressing statement or you might say, “Okay, so that's reasonable. This is real life and the Internet's very big and there’s a lot of competing forces. Let's find out where we are.”

Within that, let me now focus on the forward motion that we're making. One of the things that several of us have been focusing on is that there are some nonautomated parts of the system that need to be automated in order to make it more useful, more easier to administer, and less error prone. And so we're pushing very hard on that with my colleague—

ROD RASMUSSEN: Do you mean [DNSSEC]?

STEVE CROCKER: Yes, DNSSEC and its application across the entire domain name system. As you undoubtedly are aware, there's a DNSSEC and Security workshop at each of these ICANN meetings. There'll be one this week on Wednesday. Within those workshops, my colleague Shumon and I have been running a running panel focused specifically on the automation of the provisioning process. How do you make the right records show up at the right time? And that is part of the entire DNSSEC system that had the least amount of attention. And we're sort of in cleanup mode in a way.

So we've been running that panel. This panel is episode twelve. So that means we've been doing it for four years and tracking the progress on various things. I invite you all to come. I warn you that we run that panel at the expert level. So if you're not a DNS expert, send somebody who is and have them report back to you.

One aspect of this is the update of the so called DS record. The nature of the DNSSEC is that there's a whole chain of signatures that go from the root on down to the leaf nodes of the tree and the signatures are interlinked. And so when the child zone is signed, there is a corresponding record called a DS record that has to be created up in the parent level, which is usually the registry. And if there is a change, which there frequently is because frequent changes are not so frequent, but regular changes of the signing key is normal, then there has to be an update process. And that update process works fine if the DNS provider is part of the registrar. So the registrar has an internal DS operation. And that's the most common way that people get DNS service.

But even though it's the most common, it's not universal—in an awful lot of people and a lot of important cases, the DNS service is run by some third party or it's run internally by the registrant. And in that case there's a lack of an automated path to get this DS record communicated up to the parent. And if the key is changed in the child zone and there's no corresponding change in the parent zone, then that chain of trust is broken and anybody who's depending upon getting the signatures correct will report that it's treated like an unsigned or a broken zone and things stop working. And that's bad news causes a lot of pain and disruption.

So automating all that has been a key thing. And one of the things that SSAC has been working on currently is a report on the status of this DS automation. There is forward progress in the cc community and not so much in the gTLD community. And so one of the things that we wanted to do was highlight the work that's gone on in the CC community.

And there are some interesting interactions in the gTLD space that arise from a business rule or practice that is very specific to the gTLD community, which is this: the registrars for many, many years in the gTLD or the contracted parties have had a very, very strong attitude. I don't know how strongly it's implemented in contracts and so forth, but the attitude is that the registries must not communicate directly with their customers. With the registrants. [Our] customers don't touch them.

And here we have a technical issue that we have information that the customer has in their zone that has to be communicated up to the parent. It could be done through the registrars or it could be done around the registrars, but it's not being done at all at the moment. And the question is, well, how is that going to get done and who's going to do it and does that cause a problem? So you have an interplay between a technical requirement and a business practice.

Now, communicating DS records up to the parent is not a way of stealing customers, even though that's the origin of the rule. It's not a way of disintermediating the registrar. But anyway, that's sort of the complexity about it.

So that's where we are. We're trying to write this down carefully so that we describe what the state of affairs are and what additional technical work still has to be done and socialize all that.

Now in terms of a campaign, boy, it'd be great to have more attention on DNSSEC and we could work on all that. The campaign … I haven't thought much about it in the terms that you've credited, but one question is, do you want to focus the campaign on the end users, on the

registrants, or do you want to focus the campaign on registrars and registries who say, “This has to be done. Make it work for everybody in a smoother way.”

I'll just leave that question hanging because now I want to get to the dessert, to the surprise topic, a separate thing that I've been spending a lot of time on since leaving the Board embarrassingly six years ago now: the WHOIS situation. WHOIS was broken for years and years remained broken, is still broken.

And I'll just say, quite straightforwardly, that the current efforts in the policy development process, both in the strategic fashion of what the Temp spec is in the Phase One and Phase Two specifications and in the more immediate so called Lightweight Registration Data Request Service, reflect an awful lot of concern about the downside risks to the registrars and perhaps to the registries, and reflect, in my view, almost zero attention and support on the requester side.

So here we are at ALAC and this is an absolutely perfect place to raise that concern. It's very important to protect the privacy of registrations. It's very important to protect the liabilities of the data holders, the registrars primarily. But those concerns, although very important, are not the only concerns.

And the other side of this is that data actually is useful for a variety of legitimate purposes, from everything from security practitioners and researchers to law enforcement to intellectual property attorneys trying to track down fraudsters and infringing sites, et cetera. And that adds quite a bit of complexity to how do you design not only the technical systems but the business processes and the practices and the

oversight and governance of all of that so that it actually works and works well?

And I'll just be quite unrestrained here and say it is quite embarrassing to be in an environment that is internet based that we can't do better than we're doing. This is just nonsense. And if we're going to have a campaign put together, a campaign that gets the people who need the data and can use the data and who will respect and adhere to proper processes for vetting who they are and what they're going to do with it, and accountability if there's a screw up and so forth. But that side of it, in my estimation (and I've been sitting in these meetings for years now) has not been adequately represented. And if we're going to have a campaign, let's start here.

JONATHAN ZUCK: Okay, you have successfully derailed the topic of discussion here, but obviously this issue of WHOIS and data accessibility is something that's discussed within the At-Large community a great deal. So this didn't come as a big shock. Alan Greenberg, who made his way from the backseats to the table (purely by coincidence, I'm sure) and Hadia were both participants on the Extinguishable PDP.

So I think that we are aligned in your concerns and more than happy to have a conversation (it feels less like an SSAC conversation) about what an effective campaign on this topic might look like. It doesn't immediately pop into my head what that would be, what the pressure points are, or what the way the path forward on that is. I mean, at this point we're talking about trying to get the requesters to even use the system sufficiently so that there isn't the ability to say, “See? It wasn't necessary after all,” or something like that. Even though they might

believe they're not going to get anything of value out of it, they need to use it anyway as a rhetorical point. And so that might be a campaign to some extent, which is to mobilize requesters to use the system that was in place.

But I'd be curious what popped into your head as being a possibly effective and user-based information campaign for that topic.

STEVE CROCKER: Thank you. The first thing is to straighten out the language. It's not the “extinguishable”; it's the “everlasting” policy development process in in the lot of personal opinions here. There’s a lot of opinions, as as I'm sure is obvious, but what I've observed is that the consensus process that's been operating in these working groups in the GNSO have certainly had voices (your voices among others) that have expressed various needs. They've been smushed. They've been sort of overrun and then consensus declared.

So there's an imbalance in my view. But the imbalance is two parts. One is structural, which is worth some discussion, but the other is the contracted parties are much better organized and consistent and persistent.

So to your question about—

ROD RASMUSSEN: Have you met Alan and Hadia? [inaudible]

STEVE CROCKER: Yeah, and I mean no disrespect. I've known Alan for a long time. We've interacted with Hadia. And I'm not trying to say anything negative about you, but the syndrome that I see is individuals speak forcefully, get overrun, and then we need to raise the level. Group need to have some energy behind it that says this is just not tolerable. We have to say what you need.

So one specific thing. So here's the thing. I don't know of any document that lays out in some detail the various modes of use that you need and what you're going to use it for in a public statement that is comparable to the public statements that come on the other side that say well, here's our concerns and legal liabilities and so forth. And they're very clear. They say there's got to be a purpose and we have to decide whether or not that purpose is something that meets the legal requirements and so forth. But there should be greater weight. I'll just leave it like that on the side of expressing what's needed.

So I'd like to see some (what's the right thing?) civil action by requesters, in whatever form is appropriate, but organizing perhaps by kind of topics. So even law enforcement people who are semi-organized and more specific than any other group I've seen don't seem to come in force. But I don't see why there isn't. Great emphasis by the intellectual property attorneys, great emphasis by security practitioners, great emphasis by the business community that needs access to that data for merger and acquisitions or other business things, all of which can be done in ways that are respectful of the privacy and accountable and manageable within the law.

And I don't see a lot of support, frankly, from ICANN Org on this. I see a lot of emphasis on ICANN Org on how to protect ICANN.org from taking any responsibility. And then they add to that how to protect the contracted parties from taking any responsibility. Okay, so that's what we're dealing with here.

But ALAC is in principle, where the other voice, a sort of a broad based other voice, ought to come from. It's not a trivial … I don't mean to make light of this. There are some serious complexities. It's not going to be a one size fits all. You're not going to get a uniform legal basis for things. But the rest of the Internet has been built and operated very successfully with a wide variety of environments and differences in legal structure and so forth, and the stuff that works. And you don't have the same rules everywhere for everything, but you can sort it out. You can tear the pieces apart.

I apologize a tiny bit, not much for having dropped in here and I didn't quite realize what we were going to talk about, but I did realize well, okay, I know what I want to talk about.

JONATHAN ZUCK: Well, one thing I'd like to do is … And I know that you've energized a few of our more vocal participants in this topic. I like that. It's a good thing. And I think that it's great when people leave the Board and have their chip removed and speak their mind.

STEVE CROCKER: I don't know what chip you're talking about, but I still have a couple of chips here anyway.

JONATHAN ZUCK: So that's always a good thing. I don't think it will take much for us to be reinvigorated on this, especially with such a good partner in crime, to figure out what the path forward on this might be.

I think what I might want to do (and I apologize) is get back on the agenda to make sure that the SSAC is able to deliver the information that they want to deliver in this mean, let's not let this go and let's not let this opportunity go. We've had Steve on calls in the past, and let's look at what we might do as a mobilization campaign around this. Again, I don't know obviously, what that is or who it is we'd be mobilizing and to whom we'd get them to speak. I don't know what the call to action would be, but let's have the conversation. I'm going to just say let's not do it in the SSAC meeting, but let's do it. I'm game. All right? So I apologize. I just know we could take the whole time on this.

Thank you, [Greg]. Don't bite your tongue. You're going to need it later. We need to keep the puns coming. So I appreciate that.

On the issue of DNSSEC, I also want your partnership. And again, it's the same question. In other words, is there a message, and users would be the right ones to deliver, and if so, to whom? That's the high level question associated with DNSSEC, but I want to discuss that further with you.

STEVE CROCKER: So let's divide the users into those that have domains that are registered (so those domains should be signed and have a DNSSEC service) versus users who are on the using domains, making requests

and so forth. I think in both cases, what we want are for those users to say, “It's important for my zone to be signed,” and for the other users say, “It's important for the ones that I look up for those zones to be signed and for the signatures to be checked.”

JONATHAN ZUCK: Who do they say this to?

STEVE CROCKER: And they say that in the second case, to their service providers, to their browser. First and foremost, it's the browser that causes the checking to be done or observes whether the checking is being done. There's some complexity about how many different signature checking processes exist within even one computer, whether it's in the operating system, whether it's in the browser, whether it's in the mail system, et cetera. But it’s to say it's important to know what the providence is of that information that is being delivered, the domain name information. And so that's a question that can be asked directly and with some vigor to the broadest.

And on the other side, they’re having their zones signed. So those would be the targets.

JONATHAN ZUCK: [inaudible] see what we can do there, but I'd really love to put you in charge of the microphone to get through some of the things. We'll [skip zip] for now and go through some of the papers.

STEVE CROCKER: I was going to say is that my membership in SSAC is [inaudible].

ROD RASMUSSEN: Yeah, we do give Steve a little bit of latitude as Chair Emeritus. But yeah, that was interesting. There was nothing official in the SSAC position there, but there's probably a lot of sympathy for exactly everything you said. Anyway, we've worked on this stuff, all of that he was going on about, for years, and we shared his frustrations and the war stories, the EPDP and all that good stuff.

I do want to say on the DNSSEC outreach stuff0 that I think, to be constructive with this, if you guys are putting together planning for a campaign, I think, if we can tailor it, we can niche in or put together some sort of a "here's what we're trying to do" and ask the SSAC, "can you provide us some good messaging on this?" and work on messaging on that and who actually to try and target and things like that. I think that's a collaborative process and maybe we can get some volunteers to collaborate together and focus that down. So I would say … I'll hand this off to Ram too, as one of his projects. So I get to make all kinds of promises. Here you go. But I think that's worth exploring, right? And that's something a liaison can help with as well. Just noting that.

JONATHAN ZUCK: Exactly. Let's have people put that together. I mean, I learned from Paul McGrady about the concept now of small team plus. So if you drive a pickup, putting a small team in your tank is enough. But if you're driving like a Mercedes or something, you need small team plus to really get

that up and go. So we'll get that going and circle back on that with a small team.

ROD RASMUSSEN: So I got more good news for you. Is it like the next four slides or what Steve covered already on the DS automation? He's taking your time with our stuff.

JONATHAN ZUCK: That's all right.

ROD RASMUSSEN: Steve, was there anything you wanted to add on the DS automation that you didn't already talk about in your prior …

STEVE CROCKER: So Peter Thomassen has been co-chairing the DS automation work party. And so let me turn it over to you, Peter. What more needs to be said? What would you like to add?

PETER THOMASSEN: Not so much. Perhaps in response to the earlier question which messages users could send, I think if you own a domain name, you could ask, if you want DNSSEC, your provider to do it, and then when they say, "Oh, we can't do it," tell them that others are doing it and that it can be done, and ask them why they're not doing it and perhaps even change your provider. So I think some pressure doesn't hurt given that you want to support the [cost].

ROD RASMUSSEN: I was just going to add some more context and I'm happy to have folks take questions. This work party is in basically final review stage within the SSAC. We have brought in outside experts on this because of the nature of highly operational nature of this who have been taking part of the work party and we've done a preview to folks, to at least some outside parties, as to what the draft looked like. We got more input and have taken that on.

We are right now trying to calibrate the level of and types of recommendations we're going to give because there's a lot of stuff that's still out there. The IETF is working on some things in this area. It's not baked yet as far as how you would handle some of these automation things. And there's debates about is this the right way to do things or not. So we're having a little kind of our own internal struggle on figuring out exactly how to say this at the right level where we can get everybody on board to say, okay, we all agree with that.

So as soon as we get done with that process, this thing's coming out. So we're already talking about working with ICANN Comms on the process around messaging. This is definitely something that we would love to be able to somehow use and work with you guys on the messaging though, is actually some specific audiences that you will only have some reach to.

JONATHAN ZUCK: Right. I mean, we're not going to have an end user message for everything that you do. For sure.

ROD RASMUSSEN: Yeah. If people have questions about this DS automation thing, we've got Steve and Peter here. So if there's any questions on that.

Okay, so then let's go ahead and move down to the Registrar Name Server Management Work Party which is a month or two away, hopefully, from being able to be wrapped up. And this one actually affects registrants. And so there may be some messaging here that we want to carry through.

And [Katam], who's one of our new members, we brought in on a work party and he's now a member of the SSAC as a result. And we're very happy to have him. [Katam]. And this is his first meet ICANN meeting ever, so don't tell him about the hazing on Monday though.

[KATAM AKIWATE]: Thank you. My name is [Katam Akiwate and I co-chair the Registrar Nameserver Management Work Party with KC Claffy. So this work party started as a result of us identifying nearly half a million domains that were exposed as a result of registrar operational practices over a period of ten years, though these practices have been going on for decades as far as we have been told. And we found that not only were domains exposed to the risk of resolution hijack, but attackers were actually taking advantage of it.

And so the thing that we are trying to do in the work party is to figure out how do we protect registrants and identify different operational practices that registrars can use so that the registrants will be protected because so far the view has been, oh, the registrants need to be

responsible for looking at the name servers themselves and they need to be always on the lookout for changes that happen. And so the work party basically is making this switch where we are saying, okay, let's try and make the operational practices better so that registrants are better protected.

And at the same time we are trying to surface the burdens that it places on the different stakeholders in the system; so the registrars, the registries and the registrants themselves. Do we expect the registrants to do anything? We are adding on the side of the registrars and registries taking responsibility for their operational practices so far.

If you're interested in knowing more about what these operational practices look like, I invite you to the open session, the public session on Thursday. I'm happy to take questions now.

ROD RASMUSSEN: Questions. I believe we did talk a little bit about this last time, but as I said, we are getting close to publication and the evolution of this over the past several months has gotten us to a point where we've got a really, I think, a very good survey of things. We have gone out with some quite … I believe we did this external too. We're planning on (I'm trying to remember now) getting feedback on what we had gotten what we've done so far.

[KATAM AKIWATE]: And also we've been working with IETF on getting this standardized as an RFC, too. So that's been also ongoing.

JONATHAN ZUCK: I definitely think the at large community is in sort of agreement with you that putting this in the hands of registrants is not the right answer, especially since it's a very overt goal for this community to lower the bar for participation in the Internet and to be a registrant and things like that. So anything that makes that process more complex and more intimidating, I think, is something we would oppose. So it sounds like we're on the same page on that issue, at least in terms of the stakeholders.

Anyone else have a question or a comment?

ROD RASMUSSENL All right. Thank you, [Katam].

Next up, another paper that is in our final review process, or at least SSAC-wide review process. I shouldn't say final, because that can tend to have a couple of iterations, but on our full review process is the evolution of DNS resolution, which we've been working on for a couple years now. And it's come to, I think, a pretty good place. I'll let Barry talk about it. Barry?

BARRY LEIBA: I was going to say I'd like to speak geek, but I don't think we have an interpreter for that, so I'll speak English. As Rod said, this is also coming to an end. We've been working on this for a bit longer than I hoped we would, but we're finally in an SSAC review of the document. This came out of SAC 109, which was the document we did on DNS over HTTP and DNS over TLS, and we looked at what else we wanted to say about where DNS resolution is going. And where we wound up was looking at

alternative name resolution systems such as blockchain resolution systems and that sort of stuff. So the document talks about that.

We had a presentation yesterday in SSAC by a couple of researchers who did some research on blockchain resolution versus DNS. So we're going to pass this by them and see if we get some interesting comments and a different take that we might fold into the document or use some of their results.

But basically the document is done. It will have some connection to the Name Collision Analysis Project work, because there could be name collisions between existing uses of things that look like TLDs that are resolved outside the DNS and TLDs that then get delegated if they're the same. So there's that.

And we're advising ICANN to offer to provide a place for people to discuss this stuff if they're interested in it, with the realization that there are alternative name resolution systems that specifically are not interested in talking to ICANN, but the ones that are ought to have a home to talk about this stuff.

One of the points we make is that as people are using mechanisms to visit things on the internet that don't show names to them—they're scanning QR codes … Yeah, search engines is a big one that you don't really care anymore whether you go to ICANN.org. You just type ICANN in a search and it gets you there. So names themselves are more hidden from users than they used to be, but they're still critical as part of the system. So there's a little conflict there where the users no longer see the names. It doesn't really matter whether it's ICANN.org or X2579G.org. It still gets you to ICANN and the user doesn't really care.

So all of that's in there and like I said, it's almost done and it's mostly for information to the community and the broader community—not just people who are in ICANN, but anybody else who is interested in reading about this stuff.

I'll take any questions. Okay, so on Tuesday this is Hadia for the record.

ROD RASMUSSEN: Hadia, would you like to talk a little bit about the [inaudible]?

HADIA ELMINIAWI: So on Tuesday we have a plenary about the technological advancements within ICANN. So as ICANN celebrates its 25th anniversary, this session is made of two parts. The idea behind the first part is to showcase how ICANN is using technology in its operations, in its management, even in engaging participants in its work. So it's basically to show how ICANN is not only coping with new technology, but using it in an effective and impactful way.

And then the second part is more about the future. And it's a visionary part. So it's like, how do we see the future?

In the first part, I think SSAC … We have John Crain. I don't actually know what he's going to be showcasing, but of course, SSAC, whether in part one or part two, could come in and say "This is what we're doing." And I don't want to say we want to impress people, but we want to show them that this is not an aging organization that has passed what's going on. So of course you're invited if you have something to show.

ROD RASMUSSEN: Amrita?

AMRITA CHOUDHURY: Thank you. A question which comes is: normally in ITU discussions or even in IETF, every time now we see new proposals being pushed vis a vis the DNS system, et cetera. [There's] some work going on on that [, as] in many times it is [counter-interacted] at that point of time. But are those actors invited to these discussions to discuss well in advance how the DNS system or the evolving DNS system is taking care of the issues which they are trying to highlight through an alternative proposal?

BARR LEIBA: I'm not sure what the question was in there. What I can say for one thing is that a bunch of us in SSAC are active in the IETF. Warren, with the hat behind me, is an area director in the Operations and Management area and is responsible for the DNS Ops Working Group, for instance, which proposes a lot of these sorts of tweaks to the DNS system.

So we're well aware of what's going on. And sometimes the work parties that we spin up to write up documents come from things that the IETF has done, such as the DNS over HTTP work and that sort of thing.

Was there a further question in there other than that?

AMRITA CHOUDHURY: It's much more. It's not the IETF. I'm talking about the ITU or other places where new proposals come up which bypass the IETF and go into ITU.

BARRY LEIBA: Okay, I'm not personally aware of any work the ITU has been doing on DNS—

AMRITA CHOUDHURY: No, I think I have not mentioned it. It's not the ITU. It is member states who come up with proposals.

BARRY LEIBA: Okay.

ROD RASMUSSEN: Any other questions?

Lutz?

LUTZ DONNERHACKE: I wrote a question into the chat. Is there any progress in the last few decades that allows us to use the TLSA records in the same form as we use certificates today for business? Background of the question: In 2008 in Mexico, we had the same discussion and there was a strong disagreement to use TLSA records for anything useful simply because the infrastructure of registrars and registries cannot handle the possible fraud load which can come up if TLSA records get really the same meaning as a certificate so

BARRY LEIBA: Quickly, DANE is not being used much in HTTP as it was originally intended because of the DNSSEC issues, but it is being used in e-email contexts. I guess I said what Warren wanted to say. So there is some use of DANE, though not to the extent that we'd hoped it would be. We'd originally hoped that DANE would be the killer app that made everybody implement DNSSEC and it hasn't kicked off that way.

LUTZ DONNERHACKE: Let me clarify. The question is about the infrastructure. Do you assume that the processes between the registrars and registries had strengthened in the last few decades, that it can handle more than the current or the last few decade usage? Or do you still think that these processes are still too weak to handle such a load?

BARRY LEIBA: No, I think from an infrastructure point of view, I think we're okay. I don't think DANE would kill the DNS in that sense.

Warren?

WARREN KUMARI: Hi. I was the person who founded and ran the DANE Working Group for a while. I don't think that that's so much the concern as is that in order for TLSA and DANE records to be useful, they need to be used by browsers. And at the moment the browsers seem to have no real interest in implementing that. So even if people can put in the TLSA records (it's doable), it doesn't seem to change that much load on the DNS. It's just that they're not particularly being used in the HTTP world.

But as Barry said, they're being used a whole bunch in mail. So that's sort of one of the examples where DNSSEC is providing something useful.

UNIDENTIFIED MALE: Maybe I can add to the response. So if you want to track numbers on TLSA for email, you can go to DNSSEC[minus]tools.org. And there is a link for statistics at the top. And it shows currently that there is about 23 million registrations with DNSSEC in general and 4 million of those, which is like one sixth, has email host names that are protected with DANE. So that is actually a number that's higher than I thought.

If you want to play around with browser stuff and if you want to write a proof of concept, I think you can start off from RFC 9102, which tries to solve some of the latency issues there.

JOHN LEVINE: I'm John Levine. Also the problem with the browsers is that they think it's too slow. They can validate a certificate signed by a CA. They can validate entirely offline because the browser has its own built in list of signers. To check a DANE certificate, it has to do a DNS lookup. And browser people have told me that it take an extra 10th of a second, and they say that's too slow. They're incredibly sensitive to how long it takes from when you click until the image appears off the screen.

So it's not an issue of capacity. It's an issue of speed, which is kind of like a speed-of-light thing. So I don't think that's likely to change soon.

ROD RASMUSSEN: Okay. I think we're going to move on to the next bit so we can get … I think we have enough time to get through everything here still. We got 15 minutes left. I believe it's at the bottom of the hour, right? Yeah. Okay.

So we wanted to bring this up here, given the spirit of alignment we tend to have. And given the prior intervention by Dr. Crocker when we're talking about things being fit for purpose, we have a prime example of an ICANN process that has delivered something that is not (at least I believe in the SSAC and ALAC and GAC and others' opinions) official opinions that we've sent to the relevant parties and the board, et cetera. It's not going to do what it is intended to do, which is get information about registrations to those people looking for it in an efficient and lawful et cetera, et cetera, et cetera, way.

So this kind of has prompted some thinking on our part. And we're going to have our discussion with the Board focusing on this, on how do we make sure that, when we go into a policy making arena or providing recommendations, as we do as advisory committees, we're thinking about … Are we offering up suggestions that will actually work? Fit for purpose is kind of an engineering focused way of saying that. But that's the bottom line: do we actually measure this as an objective criteria for an output of a process and is there anybody to actually check that work, so to speak, because we now have examples. I would say that the RDRS system may be one of these. We have the whole concept of an urgent request that may be a matter of life and death being—

UNIDENTIFIED MALE: Seven days.

ROD RASMUSSEN: Three business days, which turns into seven days that does not seem fit for purpose or effective—

UNIDENTIFIED SPEAKER: If the purpose is to save a life.

ROD RASSMUSSEN: If the purpose is to save a life. Yes, that's true. Depends on your purpose.

So this got us thinking a bit about this, and we've kind of reframed this a little bit from how we originally brought it up because we realized that this actually gets into kind of a larger thing that we've always thought about a bit: integrating successfully SSR considerations into the process here and aligning that with the global public interest framework, which is something that is a current focus for ICANN.

And can we think about this from the perspective that these thing … It's like security built by design or security by design kind of principles in that everybody needs to be thinking about it and the SSAC can't think about everything. We don't review every policy that's put out there. It's not our job to do that, and we're not physically set up for it. We don't have the people time, et cetera. We're volunteers that look at specific issues mainly in the long term that can affect things and make sure we're steering away from hitting continents, not individual icebergs. Right? So how do we do that in a better way as an overall community? Because it is part of the overall mission statement of ICANN: the stewards of the naming system. So this gets kind of into fundamentals.

Can I have the next slide, please? No, that's one. Okay. Brainstorming questions. There we go. I'm sorry, I was looking at my own presentation, not the one on the screen. Sorry. So we've actually been taking a look at the global public interest work that's been done recently. And so some of these we're trying looking at fitting this in here, because that seems like a logical place to be thinking about these kinds of issues in that if you're going to be working on policy and doing things, at some point, you should have some sort of thought that whatever you come up with is actually going to do the thing you want it to do. Right? It's implied. If you read the language, it's kind of implied that, oh yeah, we're going to build something that will work. But we don't say that, and we certainly don't say how to measure that or where along the process that happens. And so what we've ended up here with is I think we've spent a lot of time doing things in ICANN world that we put tens of hundreds of thousands of probably of volunteer hours into. And at the end of the day, it ain't going to happen. So how do we avoid that further up the chain. Right? So that's kind of the meta issue we're talking about.

That's why we had this idea of … We're starting with the engineering view of fit for purpose as an output. But this basically cuts into, should we do things that are effective? And that's why I think one, two, three the fourth bullet point here … In that public interest framework work, there's a perfect place to add this potentially, which is the word "effective." It was just kind of synonymous with built fit for purpose in a phrase that's not so engineering techie, but it's basically like, will it do the job? If you think that's an important aspect, okay, where do we build this in? Is this in the policy making thing? Who owns this? Is this

something that any PDP, for example, should be checking as it goes through before it publishes things? Is there somebody who needs to be taking a look at things as they come in? We don't know. This is discussion that we should have.

But our opinion (this is fairly unanimous, I think) is that we should have this as a kind of table stakes to doing anything that is going to be implemented: it should actually do what you want it to get done at the end of the day. And there's a whole bunch of aspects to that and it's going to be dependent upon what the thing is that you're making a policy about. But certainly any stakeholder affected by the policy and anybody expected to abide by the policy should be part of the consideration. And is it practically feasible to do? In other words, if I propose something in faster- than-light travel as required for it, it's not currently feasible as much as we like it to be. And I think that we've come to that with the WHOIS question. We need time travel or something past the speed of light to make this work and I don't think we want to be there.

So that's what we wanted to kind of talk a little bit about here and see how that aligns with some of the things you might be talking about internally. I know you and I have had a little bit of conversation about that, but I wanted to throw that out there and maybe do a little quick brainstorming for a couple of minutes and see where we might take it from there.

JONATHAN ZUCK: Yeah. I don't know if you're aware of this, but I have from time to time brought up the issue of metrics in the context in the ICANN community, and in fact actually chaired a PDP at GNSO, launched PDP on metrics,

the result of which was rewriting the template for the charter and the final report to include sections on metrics. The degree to which that's taking place is another question, but I will say that I'm seeing the word come up more and more. I know in the GGP work on applicant support, for example, there's some fairly significant work on metrics. And to me there's a big overlap in that when you talk about something being effective, that's probably a function of defining what you mean by effective in each case and doing so in an objective enough way that you can measure effectiveness because otherwise it's an abstraction.

And so then I find my way back to metrics when all is said and done: I'm coming up with measures of success essentially for a particular policy implementation or technology or something. But we need to build into this.

And the other term that's coming up more and more these days is something called continuous improvement. That suggests that if something isn't working, we can stop doing it or improve it or make a course change. And while being age old concepts in the rest of the world, they are still fairly nascent here.

So I personally think that we're well aligned with that notion, and then it's just a question of figuring out how that would be, because adding the word there to the of a public interest toolkit probably isn't going to get it done. So we have to figure out really what it means to be effective and have a process for defining the effectiveness of a particular initiative so that that effectiveness can be measured.

ROD RASMUSSEN: I would say on that that adding the word is necessary to get people to actually start thinking about doing that other bit because I find that if it's not written down somewhere to start it, nobody's going to do it right.

Do we have any—

JONATHAN ZUCK: Alan Greenberg?

ROD RASMUSEN: Alan? Yes. There we go. Alan?

ALAN GREENBERG: I guess thank you for bringing this up. I think there's a huge overlap between what you were just discussing here and what Steve was discussing and this whole concept of if we build something, does it have utility? Is it meeting a need? And part of the answer is who's going to measure the need? I mean, if you build something for shipbuilders and then have it inspected by someone who builds toys and they decide whether the shipbuilders are going to be satisfied or not, you're not likely to get a really good answer. If you're building something for shipbuilders, perhaps you should ask the shipbuilders whether it helps them or not. And we don't do that here.

I could talk at length about SSAD and how did we decide that SSAD was fit for purpose in the recommendations and it was with the complete disagreement of the people for whom the system was for. It makes no sense. There is some structural problems in how we make these

decisions. It's not so much that we don't try to make the decisions we do, but we make them in ways that don't make a lot of sense. And someday we're going to have to address that issue here.

ROD RASMUSSEN: Let me offer up another example that was brought to my attention today because it was something we mentioned in a different meeting. As a potential future work product, we were going to take a look at the EBERO process, which is the emergency backend registry operator. So in other words, if a registry fails, the TLD is supposed to be caught by somebody else and kept alive. Well, let's just say that a registry operator who is very familiar with this territory is like, "This thing is completely broken. It does not work. It cannot work. Not the way it's done."

So there's another thing, and this is for a contracted party to be able to take on. Right? This is not external. This tells me this is a problem that's ICANN-wide. It's not just not listening to end users.

So how do we kind of prioritize this? And I think it's a good time to do it while we're talking about the strategic planning and all that stuff. This is a nice time to be able to start thinking about … And the continual improvement process, because this is part of continual improvement. It all fits right in.

JONATHAN ZUCK: You want to fit it under the branding of what's going on.

ROD RASMUSSEN: Yeah. “Hey, how do we get our idea a little bit more palatable to Board?” “Oh, yeah. The public interest. That's right.” And getting things to actually work.

JONTHAN ZUCK: [inaudible] plus.

ROD RASMUSSEN: Yeah. There we go. We can get all the buzzwords in, but at the end of the day, it's all about making this thing work better.

Alan?

ALAN GREENBERG: If I can try to encapsulate a problem, we are far more focused on process than end results. If we follow the rules, if we follow the process we wrote down or someone wrote down, then it's acceptable regardless of the actual outcome. And I think it applies to EBERO, it applies to Sid, it applies to a whole bunch of other things. Thank you.

JONATHAN ZUCK: We've hit the two minute mark, probably. So we probably need to wrap this meeting up or—oh, you've got one more slide you want to roll through?

ROD RASMUSSEN: It's an important one. Two slides down. Yes. One more. There we go. So this is the last one of these that Julie and I are going to be doing at the

front of the room. Well, thank you. You see us smiling, though, don't you?

JONATHAN ZUCK: You're going to miss it.

ROD RAMUSSEN: Yeah. I can still hang out with you guys. That's fine. Ram Mohan is going to be taking over his chair and that's as of January 1. We do ours on the calendar year. So you can still bug me for a little bit and I'll bug you for another little bit here, John. But anyways, so we'll be doing that transition. Tara Whalen is going to be vice chair. Tara is here. There we go. Congrats. And because our shoes were so large … No, actually there was a very good idea by some of the folks that were interested in leadership to say, hey, let's actually join the Admin Committee and help out. So Barry Lieba, who's here in the front, and Jeff Bedser … I don't know if Jeff … But you all have met Jeff or many of have. They are going to be helping out on the Admin Committee as well. So some of these initiatives and things like that they may be asked to head up. And then, as I said, that begins on January 1.

I already mentioned the transparency thing, so that was the other part of this. So there we go.

JONATHAN ZUCK: Thank you. That was very transparent. And we thank you for all of your work. The two of you have been great to work with. And we look forward to working with Ram and Tara.

And thanks, everyone, for coming to this meeting. And it looks like—

UNIDENTIFIED MALE: [inaudible]

JONATHAN ZUCK: Oh, yes, sorry. And thank Andre for his time. I don't know, I thought we'd already said something.

ROD RASMUSSEN: And we get to keep them too. It's great.

JONATHAN ZUCK: Yes, and we have a new liaison as well, [Matthias], so that's going to be great as well. I focus too much on results and not enough on process.

Thanks, everyone. We have a lot of takeaways from this meeting, as always, so I think we have a lot going on and we're making Steve an honorary member of the At-Large community and we'll work on a number of different initiatives as a result. So, thanks, everyone.

Thanks, [Rod]. Thanks for all your good work.

[END OF TRANSCRIPTION]