ICANN76 | CF – Joint Session: ALAC and SSAC
Sunday, March 12, 2023 – 13:15 to 14:30 CUN

ANDREI KOLESNIKOV: Hello, my name is Andrei Kolesnikov. I am a liaison in SSAC, and while we are waiting for Jonathan to appear here on stage, let me just go quickly through the agenda of today's meeting. I don't know, it's being recorded and broadcasted. We haven't started yet. All right. Here comes … Yeah!

YESIM SALAM: This session will now begin. Please start the recording.

ANDREI KOLESNIKOV: All right!

YESIM SALAM: Hello and welcome to the joint session ALAC and SSAC. My name is Yesim Salam and I'm 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, Spanish, and French. Click on the interpretation icon in Zoom and select a 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. If you're 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, ALAC chair; and Rod Rasmussen, SSAC chair. Thank you.

ANDREI KOLESNIKOV: All right. My name is Andrei Kolesnikov, I am ALAC liaison to SSAC and I'll be very brief to save the time. So we have a traditional meeting between ALAC and SSAC and it has two blocks: issues of ALAC, issues of

SSAC, projects of SSAC. So let me pass the microphone to Jonathan Zuck, ALAC chair; and next will be Rod. Let's begin.

JONATHAN ZUCK: Welcome, everyone, and apologies that I was the one that was late. I forgot what floor we were on, so I was running around downstairs.

Welcome, everyone, to what has become a regular and I think very rewarding interaction between the SSAC and the ALAC on a variety of issues. I think we find ourselves aligned more often than not on a lot of issues and we always take this opportunity to [inaudible] the SSAC to be more assertive in the ICANN world and not hide behind their publications. So it's always a good meeting.

But we're excited to have you guys here and to talk about the work that you're doing because it's always important work. We're going to talk about a couple of things. One is a letter that we sent with respect to these ICANN accreted … I don't know exactly why this is on the SSAC schedule but it got there. So a letter that we sent with the BC and the IPC with respect to the contract negotiations that they're having with the contracted parties and we can talk a little bit about that.

Then we want to talk about some of the operational concerns with SubPro and talk a little bit about DNS abuse because in a previous meeting we had talked a little bit about trying to come up with a DNS abuse road map of sorts and I think that's become that more pressing. There's definitely an indication from the board and new management at ICANN that they want to set a deadline to really start to begin subsequent procedures. They want to get a date when that's supposed

to happen. Rod and I saw that same pressure in the meeting that we had, the SO/AC chair meeting. But that's the number one question on the board and Org's mind is when will this new round start? So that has an opportunity to be useful to us, because if there's a deadline, then it creates action where there might otherwise be inaction. So I think that's part of the upside of a date happening. So we'll talk a little bit about that in the context of DNS abuse. I'll give you a second [inaudible].

ROD RASMUSSEN: Well, thank you, and thank you for having us again. It's always one of our highlights is meeting with the ALAC and having some good discussions and frank discussions about what's going on. I will channel Steve Crocker and say our publications stand on their own merits but we are happy to talk about them and expound upon them, etc. But hopefully they do stand on their own and are persuasive. But as we know it's always good to have some allies, etc., supporting the things you're trying to accomplish to make the Internet better, safer, etc., for everybody.

JONATHAN ZUCK: Thanks, Rod. So, again, I confess I don't know exactly why we put this first thing on our agenda for the meeting but we did sign on to a letter that I think was composed potentially inside of the IPC but the BC and the ALAC signed onto it as well. And the ultimate premise behind it was that the contract negotiations back in the early part of 2013 through 2016 had a lot more kind of community input. There was a call for priorities. There was a community review of the proposed amendments

to the contract and I think there was something like 75 of them, which may be part of an answer to our own question.

But this particular negotiation between ICANN Org and the contracted parties was meant to be a very look at contract compliance's ability to get more specific requirements out of the registrars and registries as far as how they respond to complaints. Before, it was vague. They just had to have a policy. So it's about making it more specific. So I think there's a desire to see if there's more within that contract that could be made more specific without even asking for more but to take people's intentions and get them into the document itself.

Philosophically, I think it comes down to a fundamental issue that requires some thought, which is when Org gets involved in a contract negotiation with the contracted parties, are they negotiating on behalf of themselves as an organization, as a company, as a non-profit or are they involved on behalf of the community? Are they our representative in that contract negotiation or do they exist as an entity themselves and it's really just a bilateral? And I think that's one of the conversations that probably needs to be had around the community and with the board to understand fundamentally how that's discussed.

ROD RASMUSSEN: You guys sent this over, so it came out of you guys, but I understand I think that because we've been focused on DNS abuse across the community, that this is an area of intense scrutiny, if you will. Both of our organizations have made recommendations in this space. Hearing through the grapevine, I know that SSAC 115 has been looked at as part

of what they're using to base some of those negotiations on. We don't know when that will come out.

I think what we all have an interest in is where this ends up and what those measures look like. Then taking from that as a foundation, building upon that and looking at ways that a) improves things and b) can be improved upon.

So, I think more at this point, we're let's see what happens with this negotiation. And I think there's a separate question around the governance issues, etc., that you just brought up that's regardless with the topic involved.

JONATHAN ZUCK: That's right.

ROD RASMUSSEN: Yeah. And that's something I think that we continue to discuss at the SO/AC coordination level and with the board.

JONATHAN ZUCK: Yeah, I think that's right. This is more of a governance issue than it is even specific to DNS abuse. It's really about on whose behalf or is negotiating when they get into these contract negotiations and I think that perspective is very important. And we should continue to discuss it around the community.

But I think, unless there's questions about that and about that letter that you guys have, then I would move on to Justine's presentation on the SubPro specific recommendations that were made. Yeah, go ahead.

ROD RASMUSSEN: I just have one more comment on this is that—and this kind of gets into the picket fence issues as they're called in the ICANN world, and having experience touching the picket fence in the past, it's very hot, so we must be careful on that. But I see that this is a little bit of a potentially a change in perspectives; I don't know. But again wait and see is what I'm taking.

We tend to make sure that our advice is written so that it is clear that it is up to the people implementing the advice to choose the instrument of their implementation versus policy, contracts, whatever it is to focus really on what the goals of the recommendations are.

JONATHAN ZUCK: Any questions and comments from the table? I don't mean to cut off conversation if you want to talk about it more.

All right. Well, I think that's going to be an ongoing discussion for sure about the contract process and I think this will come up again closer to a new round that will probably be additional contract negotiations at that time. There is always that distinction between whether it's going to be a policy question through a PDP or it's going to happen via contract amendment. And I think at this point we're looking less for new stuff in the contract and more about clarifications in the contract

because I think new stuff probably needs to come through the PDP process. Questions? Any other questions? Anything on Zoom?

All right, thanks. So, the second thing, we did have some correspondence with the board that we did as correspondence and not as formal advice with respect to the operational design assessment. I mean, there were a number of issues that came up and so some of the issue has to do—and we actually have a session coming up with this about the ODA/ODP process and reviewing it. Now that we've had two of them, what are the cracks in that system? What should be different, etc.? And what should we focus on?

So, as we scroll through this, we were looking at areas for further discussion I think is needed. Problematic assumptions made in developing the ODA and new issues raised by the ODA. I mean, one of the bigger issues was this sort of option one, option two concept that was a pretty wide gamut, right? Five years to 18 months, $500 million. I forgot what the other number was at the low end. A lot smaller though, right?

So there is this question about what level of automation there should be. I don't know if you guys were in the session this morning about subsequent procedures whereby Becky was saying that they have to find some balance between a purely manual process that can't handle all the applications that come in and a purely automated process that's so expensive if there aren't enough applications. So that was one of the things that the board is trying to consider to find this middle ground between these two solutions.

I think, separately, some exploration needs to go into the numbers themselves and why in fact they were as large as they were and what does that number convey as well?

But one of the things that we talked about with them in the DNS abuse side, and I guess this sort of blends into our next conversation, is really looking at the idea of metrics on DNS abuse and I think right now I feel like this conversation happens in the abstract a lot. We're trying to say there's lots of DNS abuse, they're trying to say there isn't a lot of DNS abuse or DNS abuse is going down and some statistics have come out. Possible metrics have come out of DAAR and some statistics have come out of DNS Abuse Institute for identifying the numbers that we might want to use when talking about it. And I'm wondering if you guys have had conversations internally about either of those proposals for how to turn this into a quantitative discussion and less of a qualitative one and where you are, what your thoughts were on that.

ROD RASMUSSEN: Sure. I do note, I think there's at least one hand up already. I don't know if you wanted to address that. Hadia, I believe.

HADIA ELMINIAWI: Hi. This is Hadia Elminiawi for the record. It's about the previous topic. Just commenting, you said that the previous topic, Jonathan, about when we were talking about new contracts. Yes, contracts would include actually community developed policies or would enforce community developed policies, but he also mentioned what if we need

new—do we need new policies? Do we need new measurements in place?

My question here to SSAC, do they think that there are further measurements required that currently do not exist through existing policy recommendations?

ROD RASMUSSEN: Measurements of what specifically?

HADIA ELMINIAWI: In relation to DNS abuse.

ROD RASMUSSEN: Oh, okay, well—

JONATHAN ZUCK: Well, that's what we're talking about then.

ROD RASMUSSEN: We're on the same page, okay, good. I was deferring on that. So, a couple of things on that. We've had multiple recommendations around metrics, etc., for looking at across the spectrum of SSR issues, DNS abuse being one of them. SAC59, SAC114. SAC114 in particular tied that towards understanding abuse that occurred in concentrations of TLDs in the 2012 round. So those are things we've already said that we should be understanding root causes and things like that.

Now, in those particular SSAC documents, we didn't get specific metrics, like a list of metrics, like look at this, look at the temperature, look at the air pressure, look at whatever. I use non-DNS terms to clarify that.

This was more a recommendation around bringing the right folks together to understand and create that set of metrics to look at.

There are certainly inputs we would have to that process if we were able to convene such a group and OCTO has worked on some of this stuff as well. In fact, they've done a really interesting and good job of taking a look at some of the things. They're going through DAAR and other activities they've had looking at DNS abuse. So there's I think a lot of stuff out there.

We actually just sat through a presentation from the DNS Abuse Institute where they were showing some of their new metrics and there were some really clever things they were doing as well. So I think there's a lot of know-how and ideas throughout the ICANN community on how to get a better handle on these things and measure them.

The other part of measuring things is what do you do with those measurements? What do these metrics mean? And that gets a little bit more difficult to decide. So in the case of DNS abuse, what is a good target? If you have a bunch of metrics, what are the targets for those metrics and how do you incentivize or have things tied to those targets? That's a long conversation but it needs to happen. I think we're agreed on that. So the question I think we have in front of us is what kind of efforts and who should be undertaking them in order to create sets of metrics and then recommend things that you can then do with those

metrics to incentivize the behavior that you're trying to get your policy to achieve?

So that's fairly generic. I'm sorry. We can get into some of the specifics too. I think that was part of what we had on tap for some of the presentation because we do have some of that. It kind of folds into this. I don't know if you wanted to take some more questions or we're going to dive into that.

JONATHAN ZUCK: You can all hear me. If there's any open mic in the room I'm sure I'm being heard. So, thank you. Yes. If there are other questions about this issue, I'd like to take them. I was just curious whether you guys had begun to think about this issue of the metrics and the targets because I think that's going to be a central discussion that we're going to have about subsequent procedures and whether or not there's sufficient relevance to the new round for any of this work to be a prerequisite to a new round or if it's just something that's happening in parallel. I think that's a big part of the discussion is what, if anything, do we need to do—and this is part of the conversation we're talking about on DNS later on is what if anything needs to be done prior to accepting new applications, I think as well right?

ROD RASMUSSEN: Yeah and an overall strategy for DNS abuse, not just with the new round but in general. We do have some … So there's upcoming … And maybe that'll help as well with some more specifics. I think that also one of the things we talked about yesterday is where this fits in the process. When

do you need to develop metrics and control measures, etc., as part of this process? Does it need to be done now or does it need to be done in parallel with other work? Just like everything else, there's dates of applications, there's dates of accepting things and making determinations and there's dates that things actually go into the root zone and start affecting things.

So, where along the path do we have to have certain things set up? I think we need a little bit more rigor in having the activities defined towards those goal dates, so to speak. And we talked about that yesterday.

JONATHAN ZUCK: I guess I'd also ask you guys if there are other findings in the SAC002, for example, that you think that we might want to take on as prerequisites, other security related issues that aren't DNS abuse that we should take on as some advocacy for from the standpoint of being prerequisites to a new round?

ROD RASMUSSEN: Right. We have specifics in SAC114. I don't remember them all off the top of my head, but name collisions obviously which we're working on. We have a presentation on that later. DNS abuse. So those two for sure. There are a few other specific items that I believe overlap with SSR2 issues and I don't recall them off the top of my head but I refer you to SAC114. That's all we've officially said on it.

For other things, well, what do you think about this? We don't have a consensus position I can really share but there are plenty of people I'm

sure willing to give advice of their own on that, and if there's anything in particular that you think we should be zeroing in on that we haven't said anything about, definitely bring that to my attention and we can take a look at that as far as if that needs to be added to our list of things to look at. But I think we've hit the high spots.

JONATHAN ZUCK: All right. Well, I don't think there's anything more in this letter that's focused on SSAC-related issues, so I think the best thing to do would be to move on to the DNS abuse discussion that we've started to have. Since we're already talking about it, you and I talked a little bit about the data necessary to understand why there was this movement of malicious registrations into the new TLDs in the last round, because that is one characteristic that makes this round specific as opposed to having it in parallel. We have this discussion about what needs to happen before a new round versus what can be happening in parallel, one observation of the DNS abuse research that was done as part of the CCT review was that there was a flood over to the new TLDs. John McCormick who often participates in our discussions attributes most of that to pricing. I don't know where you guys felt about that issue and if there was anything in particular about the new TLDs. You mentioned that there might need to be more research there.

ROD RASMUSSEN: Yeah, indeed. There's plenty of anecdotal evidence around that. Pricing is one of the things that's often brought up. Know your customer, your measures or another. There's many various hypotheses out there. There's not a whole lot of hard data to go with and this has come up in

other conversations we just had today and we've had over the past years around wanting to understand that better. Some of this data is hard to get. Pricing data fluctuates. And besides the trade secret stuff part of that, people change prices based on volume and specials and things like that. So it's hard, I get that.

So that might be something we have to do some really interesting types of research where you don't necessarily … You have the hard data but you can interpolate and extrapolate.

But there are other things you can do as far as measures that people are actually using and that can … Other vectors for registrations or account takeovers, for example. So are you using multifactor authentication at your registrar? If not, then you might be more susceptible to your registrants getting phished and then those accounts being used to register lots of domains from people who take advantage of the fact that they have access.

Those are all things we should be taking a look at to understand root causes for where abuse occurred and why it may have concentrated in particular TLDs and that takes a concerted effort to do which is one of the things we recommend doing as part of our review of the SubPro stuff in SAC114. So I think there's a few things to do there.

I know we have … Did you want to bring this presentation up?

JONATHAN ZUCK: Sure, yeah.

ROD RASMUSSEN: Because I think this would actually help a little bit here.

JONATHAN ZUCK: Can you bring up the SSAC presentation?

ROD RASMUSSEN: We have an overlap here, so we might as well take advantage. So if you can scroll down to the sixth slide, please. Right.

This combines our long-term view with the questions about the next round because they really are, as people have said, why are worried about solving abuse in new TLDs when we should be looking at it at all TLDs? We agree you should be looking at all TLDs, but you should also learn from the past and not repeat the past when there's a problem.

The areas where we can take a look at both from a strategic plan and thinking about the next round include things around the mitigation aspects. What are those kinds of things you can do, not just in the incident response side of it but also proactively preventing it? What can you do around creating policies that makes it easier to share information? What are the goals, what are the shared expectations we have listed there of a program for the industry? So what does that look like?

Really, from our perspective, what we've started the conversation with the board with at Kuala Lumpur was around the strategic plan itself and taking it from that top level that exists today into a more fleshed-out area on DNS abuse and I think that ties directly to if you're doing that

kind of work, you can take advantage of that for looking at the next round because it just becomes part of the overall process.

And of course making baselines so that we can—and the metrics to measure those things. Also, on the flip side of this, it's not just about the contracted parties and hosting companies and others in the ecosystem. It's about the reporters. One of the big challenges that we have in this space is people of various skills, knowledge, background making reports. A lot of them are not useful or not accurate and how can you—

JONATHAN ZUCK: Reports to the contracted parties or—

ROD RASMUSSEN: So this is the people reporting incidents. Everything from a cybersecurity company with a lot of expertise that automates everything and sends you really good stuff to some individual person who has gotten a spam email and complains to somebody. So there's this huge spectrum of the kinds of reports you may receive and how do you deal with those and how do you create a better ecosystem, especially for people who are doing this at scale? So that would be serial victims, cybersecurity companies, things like that because that goes a long ways towards making the whole system work a lot better.

Then looking at this is not just an SSAC problem, it's not just an ALAC problem, it's not just a contracted party problem. It's something that we should be really combining efforts.

I personally will say I'm encouraged by all the work that's been coming lately. You've got this contract negotiation going on. You've got discussions in the community. There's a lot of newly found want here so let's take advantage of that. Then if you can go to the next slide, I think we have some specific things we could do here when it comes to the next round. We're opening it up for further expansion. And that's looking and aligning the existing recommendations we already have on paper between us, you, the GAC, the CCT review, others. I'm sure there's more around this topic.

JONATHAN ZUCK: SSR2.

ROD RASMUSSEN: SSR2, yeah, that's a good one. And see if there's a way for us to—and this is create and combine statement but at least a combined talking point because we typically have separate documents—that we could align on as far as here's what we think really are the things to concentrate on, whether that's metrics, goals, potential mitigation activities, etc. Is there a way that we can work together and in conjunction with the full community around that? But we do have that opportunity to do so and there's a lot of interest as we know from our fellow chairs of trying to get aligned and make this process a group effort rather than the board working one-on-one with each of the SO/ACs or the Org working with individually. Can we do something in a combined fashion?

Sorry for the little longwinded, but there's a lot wrapped around that topic area. I'll turn it back to you, Jonathan.

JONATHAN ZUCK: Thanks. I'd really like to turn it around to the community more. I don't mean to dominate this conversation. How do folks feel about trying to coordinate something that's a joint … We have a meeting coming up about some advice that we did together with the GAC in 2017. Things can take a long time to happen sometimes but how do people feel about trying to work together with the GAC and SSAC to … We probably have the CCT review covered because I was in it, but what about trying to coordinate those efforts? Bill, go ahead.

BILL: Yeah. I'd say anytime we can do something with allies, it's all to the good. We're going to get a lot further if we and SSAC and GAC, etc., come together to the board and say, "This needs to be done," rather than … Even if we all came separately saying the same thing, I think a joint statement is always all to the good to get the message through clearly. Thank you.

JONATHAN ZUCK: I think that's right, Bill. Other thoughts on this? Joanna, our GAC liaison.

JOANNA KULESZA: Yeah, thank you, Jonathan. I was just going to say exactly what Bill did. More concise work we are able to produce is always welcome. I understand that the GAC is setting up a small DNS abuse working group

where there will also be able to be targeted efforts trying to address that specific issue. Metrics are wonderful. Thank you very much for these. We struggled with metrics on DNS abuse for a long time and we do that on a daily basis. So the more precise numbers we have for that phenomenon are welcome. And if there is any way for us to work bilaterally or multilaterally to target, to zoom in on that issue, granted we are able to provide metrics on what it is that we are talking about, that has strong support. So that was just a reaction. You asked for reactions. It's a hurray from me. Thank you.

JONATHAN ZUCK: Anybody on Zoom who has put their hand up?

ANDREI KOLESNIKOV: No hands.

JONATHAN ZUCK: Has the SSAC at all looked at these measures that the DAAR and DNS Abuse Institute—I guess you just got that presentation. Do you feel like it's within your remit to look at those methodologies? Because that's part of it. In some ways, I don't think … Maybe with the exception of some individuals don't feel qualified as a group to make an assessment of that long methodology document that came out of the DNS Abuse Institute or DAAR, etc. So what is it that DNS Abuse Institute felt was missing from the DAAR approach or vice versa? They're all based on reputation block lists. Is that the best way to get this information? Does that feel like something that the SSAC ought to be looking at or is that too politically charged?

ROD RASMUSSEN: No, I don't think it's too politically charged. It's more a matter of what we're working on and the number of SSAC members who would be interested in digging into that and then scoping that.

Just to give you a little more background on that, we had a work party that did the work for SAC115. We had a much bigger scope for that work when we started it because we thought we were going to get into some of these things but that became too big of a project, so we concentrated on the incident response portion. And in there we actually do talk about some metrics. We talked about things about evidentiary standards. We talked about timing. We talked about escalation paths, a whole bunch of things that were actually practical and I think have, at least from the feedback I've gotten, have proved at least somewhat useful for folks that are having this discussion now. That's purely an incident response mode. We had tabled—and I believe it may be in the document that we may be potentially further considering things like preventative measures for examining registration patterns, things like that, as far as the prevention side or other things you could be doing as part of—in the cybersecurity industry, we call the kill chain as far as where you get at an event that's going to potentially happen to you.

I've been told it's time. So we're pretty much right where we need to be because I'm finishing up right now. But I think there is some potential for us to do some work here, but again, if we do a cross-community thing, that's a really interesting thing to take and we do have the expertise on staff, in our membership to do that. I just have to convince them to do it.

JONATHAN ZUCK: I feel that's where the ALAC and the GAC might feel handicapped is doing that analysis of some of those methodologies.

ROD RASMUSSEN: And then bringing in … We use our combined power to see if we can get some outside expertise to actually do a project.

JONATHAN ZUCK: All right. What's next?

ANDREI KOLESNIKOV: Next are certain projects running in the SSAC. So we'll start with Name Collision Analysis Project, please.

MATT THOMAS: Thanks. Matt Thomas, one of the co-chairs for Name Collision Analysis Project along with Suzanne Woolf over here. We have quite a few slides and only five minutes given to this, so I'm going to be brief. You can review the details on the slides here.

But essentially, the Name Collision Analysis Project was stemmed to of the board asking SSAC to study and provide some answers to a set of questions as well as some specific advice on home, corp, and mail. The work was divided up into three studies. Study one concluded a couple of years ago, which was an exhaustive and complete reference of all things name collisions. We are hopefully now in the final runway approach of study two where we are working towards consensus on

findings and recommendations. If you're interested, please join. Next slide, please.

Just some of the high-order bits of what has been discussed in name collision discussion group over the last year or so was the publication of a couple of reports. Two of them are listed here.

The first is a case study of collision strings, specifically looking at corp, home, and mail. Those strings, in addition to internal, lan, and local were also added just for comparative measures. At the time, those additional strings were receiving more than 100 million queries per day at A and J root servers operated by VeriSign.

The report looks at roughly about eight years of DNS telemetry data at the root to examine the changes of corp, home, and mail and shows that those strings have had increased query volume and diversity over time, especially with some specific growth during the pandemic in which the remote from home work elevated those critical diagnostic measurements that I'll talk about in a little bit.

The second study is a prospective study of DNS queries for non-existent top-level domains. This study was really focused on understanding the data that can be observed and used at the root server system for assessing name collision risks. It is useful for providing insights or guardrails for what data could be used and what is appropriate and how to use that data in a meaningful way for risk assessment purposes.

There is a third report that is not listed on here but it's also completed and consensus has been called on and that is the root cause report. The technical investigator hired by OCTO, Casey Deccio, studies the 40-

some name collision reports received by ICANN since 2012. His work really highlighted that there was a variety of impact felt from name collisions. Some of the impact was from minor to sever. Next slide, please.

So, some of the key findings that we've observed so far is that name collisions continues to be a problem and it doesn't seem like it's going to abate any time soon. And the main leading causes of name collisions appear to still be DNS service discovery protocols and suffix search lists. One of the things that the group has also identified is that critical diagnostic measurements, which we'll talk about a little bit here, are also a helpful way for quantifying and describing the risk associated for name collisions. These critical diagnostic measurements are a way to help describe the traffic observed for a particular string in terms of name collisions, but it only provided a quantitative, not a qualitative, perspective on that.

Finally, there is also potential opportunity for existing measurement platforms to be extended to help provide some insights to applicants into the next round in advance of submitting their application. ICANN already has the ITHI Program that has instrumented L root as well as some recursive resolvers out there that include measurements around name collisions.

ICANN has also published their magnitude page which is instrumented from the L root server ICANN operates, in which they publish I think roughly the top 1000 non-delegated, non-existent top-level domains along with some of the CDMs for those.

So hopefully those systems will be able to give some applicants advanced insights into name collisions before going into the next round. Next slide, please.

These critical diagnostic measurements are kind of outlined here. They were heavily taken from the great work that JAS and Interisle did back in 2012. They primarily focus on describing the DNS traffic observed at any point within the DNS hierarchy for that particular string, but it looks at business query volume and then diversity, and then diversity is really looked at from multiple different factors including network and IP diversity as well as query type and label diversities. Together, these critical diagnostic measurements kind of help inform what potential impact and maybe potential harm there could be for a particular string. Next slide, please.

So, the overall arching goal of this NCAP Study 2 is to really provide a sustainable, repeatable model for assessing name collisions going forward and that is to make name collision assessment risk management kind of process and that is obtaining data, studying it, and applying the appropriate risk controls to understand name collisions for a particular string. Next slide, please.

So, to that end, the discussion group is still working on and figuring out and finalizing the consensus on a proposed work flow, but here you can see what something might look like coming out of the Study 2 report.

It starts with an applicant selecting their string that they would like to submit. Then hopefully that applicant would be able to leverage the systems that I mentioned before, like ITHI or the magnitude or other

instrumented name collision repositories that have some kind of sense of potential name collision issues prior to submitting their application.

Once the application is submitted, it will go to what is called a Technical Review Team. This Technical Review Team is responsible for collecting and analyzing the DNS telemetry associated with that particular string that was applied. During that particular assessment, that is called a static assessment which is essentially the Technical Review Team looking at again data sources that were pre-published or pre-populated on some kind of mechanism to look at potential alarming or catastrophic types of name collisions. If that is all kosher, it will then proceed into the phase called Passive Collision Assessment. Passive Collision Assessment is a technique that is being proposed that facilitates the delegation of the TLD into the root and the configuration of an empty zone in which, for that string then effectively the data would be collected at the TLD's name servers, which in essence is forcing a root-wide collection of data for that applied-for string.

The Technical Review Team will review that package and information. If everything is fine, it is then proposed that it will go into the next stage called an Active Collision Assessment in which the zone is wildcarded and potential warning signs and messages are returned to impacted systems and users to alert them to name collision problems.

After that step, the Technical Review Team will package together their quantitative, qualitative assessment and send it up to the board for a final approval and then it would be the granting of the TLD to the applicant.

One of the things you'll note on the work flow is that there are the one, two, three, fours at the top and those are potential opportunities in which the applicant can have an off ramp and exit the application process due to name collision problems at any time. Next slide, please.

So this is just a little bit more of the roles and responsibilities of the Technical Review Team. I don't think we'll get into that here given our time constraints, so next slide, please.

And again, here are some of the roles and responsibilities of what we call a neutral service provider which could be the TRT or not. It could be a separate entity. Again, we'll ski8p over this for the sake of time. Next slide, please.

But at the end we are hopefully approaching the end of Study 2. Please, if you have interest in the subject, come join the discussion group. The link is there. We are working on our findings and recommendations and we're hopefully going to target a publication before ICANN77.

Suzanne, did I miss anything or go over anything too quickly?

SUZANNE WOOLF: No. Unfortunately, this is sort of a complicated situation. Lots of moving parts. And the stage of the work where we are now is that we're sort of trying to solidify. A great deal of background work has been done but we're at the stage now of agreeing to findings and then to recommendations and that's where you find out where there's still work to be done, where consensus might be weak. We're shooting to have a version four public comment for next—before 77. But there's still

some work to be done just as far as what we make of what we've found so far.

So, in all seriousness—and this is open participation effort. So if folks are interested, come talk to us. And if you really want to get involved, please we're happy to have you. Thanks.

ANDREI KOLESNIKOV: All right, let's move on. We don't see questions here, do we?

JONATHAN ZUCK: Just a quick question and then there's somebody else.

ANDREI KOLESKIKOV: Very quick.

JONATHAN ZUCK: Is there a top line here in a way? Again, it is a complicated issue. There's a lot going on. But is the takeaway at a high level that this is a manageable problem, that if they go through a process like that, then people can be a little bit more aggressive in terms of the strings that they go after even though there have been some collisions associated with them or is it more a top line that says that this is a bigger problem than we thought it was and that we really need to proceed with caution? What's the headline of this effort do you think?

MATT THOMAS: I think the headline would be that the goal of the work output of the group is to create that sustainable repeatable model to have some

deterministic behavior going into subsequent procedures in which there is clarity and confidence that name collisions will be assessed in a predictable manner in which then applicants have the confidence going into that, if that answers your question hopefully.

JONATHAN ZUCK: Bill, go ahead.

BILL: Yeah. Could we get that link to the discussion group put in the chat? Because on the slide it's not clickable.

MATT THOMAS: Sure thing.

BILL: Thank you.

JONATHAN ZUCK: Olivier, online.

ROD RASMUSSEN: The private use is a separate question. Are you asking if one of the corp, home, or mail?

OLIVIER CREPIN-LEBLOND: That's correct, yes. So, [inaudible] dot-home and dot-corp, for example. [inaudible] in the future dot-home being the result of that process that

we're seeing here, the string that will be selected for private use or has the discussion on—

ROD RASMUSSEN: Yeah. That's quite a bit premature on that. That's now over at I believe the IETF is working on … Okay, I'm getting a look from Suzanne. But we are not there yet. The ICANN process which we recently commented on is the latest bit that we've done that work on. But there is a process they proposed for determining the string that hasn't even been decided on yet. So a little premature on that.

So, two things, housekeeping wise. We have more content than we have time for. But we put extra content in here. We will [cut] from the bottom. Because what we're giving you is a preview of some of the work that we haven't finished yet which we don't always do. But since we didn't have any new documents, we thought we'd give you some of that.

The NCAP, though, this is the most important thing we've got going right now. As with the new rounds being pressured as set dates and things like that, this needs to get done. So this is really the time to be looking at what's coming out of the discussion group. If you have folks that have been interested in that but haven't participated, take a look and maybe even have somebody participate, please, because we're coming down to it. That whole process that you saw there with the potential mitigation steps where you can do more and more positive testing. That is not consensus. There's a lot of back and forth opinions about whether or not these are things that are appropriate, and this happened 13 years ago as well because SSAC proposed a lot more intervention in doing name collision analysis back in the first round.

That was rejected. There is a chance we will be proposing it again and it may be controversial. So I'm just giving you guys a head's up that there may be something coming down the line here where you're thinking they've figured out a process. There may be some controversy here, so I'm just flagging that so that folks are aware.

And I'm not going to weigh the scale which way we think it should go but I just want to flag that and this is something to pay attention to right now.

So with that, I think Russ is next—Russ or Barry, one of the two with the evolution of resolution. And maybe the last thing to do, and maybe sneak in one more after that. But you have the content of the slides, though.

BARRY LEIBA: I'll keep this brief. I understand it's 28 degrees out. I didn't realize that inside it was going to be in Fahrenheit. But I'm Barry Leiba. I co-chair the Evo of the Reso work party with Russ Housley who is two SSAC members to my right.

When we started this, the intent of this was to look at what we did in SAC109 which is the document where we analyzed DNS over HTTPS and DNS over TLS. Whether we had anything more to say about those at the protocol level, what other issues they might bring up and what other changes to the DNS resolution were coming along.

And as we started talking about it, we decided that where we really wanted to go with this was to talk about more fundamental changes in how names are resolved and how the name spaces are laid out and

what name resolution systems were coming along, like blockchain based things and that sort of stuff.

So that's what we've been discussing and we're at a stage, it's still fairly early. We actually just hit a year that we've been starting to chat about this. And we're at a stage where we've got the topics we want to talk about and we're starting to write down the details. The result of this is going to be a report from SSAC. We don't know yet whether it's going to be full of recommendations or just full of information or where it's actually going to wind up. But the idea is that we're discussing the fact that domain names themselves are less relevant to end users right now as opposed to searching for things and letting search engines take you where you want to go or letting the application itself direct you to places.

So, what changes does that make to the security and stability of things and the end user experience? That's where we are. We're discussing this aimed at an audience of not particularly technical audience. The goal of this is going to be to target it to the community at large, which we're in the right place right now.

To save time, that's all I really want to say about it right now. Russ, do you have anything you want to add?

RUSS MUNDY: Just one quick example. With COVID, restaurants stopped handing out menus and put little QR codes. Well, they actually take you to a website but you have no idea what domain that thing is associated with and

that's an example of the kind of thing that Barry was talking about, about the domain name being less relevant to the end user.

BARRY LEIBA: I guess one thing I'll add to that is the other side of it is that you can still fool people by giving them lookalike domain names and things like that. So while the users are not tending to use domain names to get where they want to go, at least as they see it. The domain names still will fool them into going into the wrong places. So there's a lot of issues there that we need to cover and we'll see where it winds up. So, any questions quickly?

Seeing no tent cards going up, thanks.

JONATHAN ZUCK: Okay. So, I think we have time for two more. We'll do the DS Automation Work Party. Peter, I think you've got a few slides here. And then we'll have a little bit of time for Julie at the end to just do a little outreach on us looking for new members.

PETER THOMASSEN: Hi, this is Peter Thomassen. Next slide. So before you look at this slide, I want to say one very basic thing on DNSSEC. The way it works essentially, you have a DNS zone, like I don't know ALAC.org or whatever and it has IP addresses and other stuff in it. You sign it, that's essentially we're adding one more record per record, which has the signature. And for that to be validated, we have to convey information

about the key to the parent domain, to the registry. And that's so far a complicated process.

So the work party deals with what can be done for making this easier and the problem is illustrated in this diagram. So, there's a bunch of arrows. It looks more complicated than it really is. We'll start with the Arrow 1. So we'll assume we have a registrant who has a DNS provider, and the feature set that he booked includes DNSSEC signatures. Then the DNS operator will put those signatures on their authoritative server as I just said before.

Now, the manual part of getting the key parameters into the top-level domain server that is above it. Takes all the detour through the registrant, through the registrar where the domain name was purchased, potentially through a reseller intermediate. Then through the registry who actually runs the TLD server; and then finally if nothing goes wrong on this way, you will have alignment between the DNSSEC parameters on the authoritative [inaudible] DNS server at the lower level and at the top level, and this includes the domain name DNSSEC settings into the global chain of trust. So this is what you have to achieve.

And currently it usually involves a manual step, which is step number three where the registrant has to fetch stuff from the DNS operator through some web interface or receive an email or whatever. It depends on the specific setup. And then transfer this information upwards in some format that is also not unified, right? There is different processes how this can be done, and it actually turn out it's complicated.

And if you go to the next slide, we found studies that say that 40% of registrants who attempt this and who do have signatures on their domain DNS records are not successful in completing this and they may have different reasons—time, motivation, knowledge that can't be expected from everyone.

And it looks like if there was automation for this step, then those who attempt to secure their domain names with DNSSEC would be more successful because they wouldn't have to do this manual step. So this is what we are dealing with.

Another consideration here is lots of stuff going on in the Internet is automated. Today you get TLS certificates automatically from Let's Encrypt, for example. DNS operation is automated. You don't have to take care of zone replication issues. Usually manually. And you don't have to renew the domain because your registrar does it. Entertainment is automated and everything is automated except you have to take care of DNSSEC. So this may be a bit contrary to registrant's expectations.

There's also other considerations which we're skipping here because I would like to focus on the user's perspective in this meeting. And next slide.

So, the goal is to develop recommendations for the automation of this kind of process of transferring the DNSSEC parameters to the parent domain and the result of it hopefully by the next or next to next ICANN meeting will be an advisory that's targeted to registrars, registries, and DNS service providers to collaborate in automated methods for getting these parameters transferred automatically in a secure way that

doesn't involve any manual steps for registrants who already have booked a DNSSEC package and who already have signed their zone, just not included in the chain of trust.

There is various specifications of how it can be done. So [inaudible] records are involved, for example, for those who want to look it up in the RFCs. 7344 it is. I'd spare you the technical details but there is a bunch of particular technical details, how the process can be varied and different registries so far have slightly different approaches and we're looking to sorting out how it can be moved forward in a unified way to make DNSSEC easier. Thank you. Is there any questions?

ROD RASMUSSEN: Looks like no questions. Thank you for that, Peter. We're looking forward to that work coming out, and again this will help registrants with getting their domains signed with DNSSEC and once we actually have this we're looking towards you guys to help us disseminate the word since you have some outreach capabilities there that we don't. So we'll get [inaudible] collaboration.

We're actually … I'm going to quickly do the next one before we send it over to Julie because, actually, I think we're back on time because we got through this quickly. Thank you, everybody. Could I have the next slide thing?

So, one other work party we've got going right now on a new interesting topic is a specific issue around name server management. This was actually released as a paper recently. This has actually been a known issue for a long time but it's one that the scale of the problem was a little

bit eye opening for a lot of folks. Over half a million domains were exposed to a potential hijacking.

The easy way to think about this is if you have a domain name, it has to have name servers that it's defined on and those name servers will usually be defined as a host name under a different domain name.

So, if you think about the fact that you've got this dependency on this other domain name, if that domain name expires or is changed or something like that—usually an expired situation—that name server host name will disappear. That creates a problem. If that domain name is in the same TLD as the domain name that's registered—so if it's example.com and it's nameserver.com, if nameserver.com expires, in that particular situation there's some protocols in place to make sure that that name server name stays within that TLD and it will continue to potentially service that original domain name.

However, if it's in a different TLD, we don't have that protection. So if it's dot-net or dot-cc or what have you, then that original domain could have an exposure where that name server domain is now available and somebody else could register it, so that new name server is on it and if somebody hits that name server when they're trying to resolve a domain, it points them to somewhere else.

So if you had a bank, for example, that was on that domain and one of his name server domains expired and somebody else registered it, they could point it at a fake bank and you would never know because depending on how many other name servers there are, every once in a while the bad bank will show up versus the good bank. That's kind of the problem we're trying to deal with.

Registrars have done different things to fill the gap in the meantime by putting other records in for those name servers and there's not a consistent practice here and sometimes they don't put anything in at all.

So what this work party is looking at is scoping out this problem trying to make sure we understand that versus other similar problems in this space and provide some advice on how to move forward with a unified plan for the industry to use as a standard for addressing this particular issue.

It is kind of a corner case thing but it happens enough that—and you have no control over it. You can monitor for it but most registrants don't know to do that. It is a problem and we want to try and help fix that. So that work party will hopefully get that done. We brought on several experts from registrars who deal with this problem that are not SSAC members that help on this work party. So that's that one. Again, preliminary stuff. Any questions on this? Hopefully I explained that enough so that folks can understand that.

UNIDENTIFIED MALE: Julie is online.

ROD RASMUSSEN: Okay. Julie, I'm going to hand it over to you to finish us off with just a little bit about what we're looking for in new members. Next slide, please. Thanks, Julie. I just pasted that into the chat as well. So again, we look to … As we're looking for more diversity, we'd love to take advantage of ALAC's reach, and please as you know we have members

of the SSAC that you guys have helped—Julie, too. They've come from you guys and we'd love to continue to that tradition.

ANDREI KOLESNIKOV: I think we're on time. Great. Thank you very much. I don't [inaudible] questions for the meeting?

JONATHAN ZUCK: Yeah, I think these conversations are going to be ongoing, and I think when there are some concrete recommendations and information, as you said, that needs to get out to the broader community, I think we are in a position to help with that. So we look forward to doing that, so thanks a lot.

ROD RASMUSSEN: Thanks for having us, again, and I look forward to … Again, I will bring up the NCAP this time to pay attention and I look forward to potentially doing some combined work on DNS abuse as we look towards both a new round and a strategic plan. We're actually going to have the conversation with the … Actually, we're talking about something different. Never mind. But we have started that conversation with the Board on the DNS abuse side, but we want to involve everybody so we'll coordinate. Thank you.

[END OF TRANSCRIPTION]