SAN JUAN – SSAC Session
Wednesday, March 14, 2018 – 15:15 to 16:15 AST
ICANN61 | San Juan, Puerto Rico

ROD RASMUSSEN: We're going to start here in just a few seconds, if everybody could find their seats.

Okay. Good afternoon, everybody. This is the SSAC activities update. I'm Rod Rasmussen, the Chair of the SSAC, and we are going to spend the next hour talking about what the SSAC is up to and the things we are looking at doing.

We have six major areas and we will be stopping for some questions in between the major segments here. We've got some time to take questions on each, but since we have a lot to cover, we will be moving through it. And there is another meeting following us, so we need to get through that.

I wanted to make an announcement up front around the Adobe Connect issue which I know a lot of you have been asking various members about. We will not be taking questions on that topic here, those would be best directed towards the ICANN security staff. There are some serious issues and those have been handled properly, and we believe that ICANN has been very prudent and has done the correct thing given the nature and the

severity of the issues that have been uncovered. So, so much for that announcement.

Okay, so that's the agenda there, and if you've got a favorite topic area, remember it's coming up when we stop for questions.

We do have new leadership with the SSAC, myself and Julie Hammer. Those are our official portraits. If you want to actually find us, look for us more like this. This is our natural habitat here, so more likely to find us that way. And we are serving three-year terms as long as we make it through. So I'm going to turn it over to Julie to actually walk through the next few slides here and describe what we do.

JULIE HAMMER: Thanks, Rod, and as most of you know, the charter or the role of the SSAC is to advise the ICANN community and the ICANN Board on matters relating to the security and integrity of the Internet's naming and address allocation system. We currently comprise 37 members, many of whom are here today and are around this table. I'm sure you know quite a lot of them.

We have quite a broad range of expertise in addressing and routing, domain name system and DNSSEC, registry, registrar operations, DNS abuse and cybercrime, Internet service access

provider and so on, but we also try and keep an eye on ICANN policy and operations just to make sure that from our perspective, the security and integrity of the DNS and the naming and address allocation systems are preserved.

Since 2002, we've published 100 publications and we continue to work on a range of topical issues. Next, please. The way we work on issues is to usually for ma work party, do some research, draft some appropriate findings and recommendations which could be for the board, could be for the community or could be for the various parts of the Internet, DNS operations community.

The approval process for all of our documents is that they are approved within the work party first but then circulated to the whole of the SSAC for review, and thereby we reach a consensus, noting that we make available the opportunity for individual members with differing views to record either a withdrawal or a dissent from that view.

When the reports go to the ICANN Board, they may or may not have recommendations to the board itself, but whether they do or not, the board acknowledges the recommendations and determines what action they need to take on the advice, and we subsequently monitor that action. And the board of course notes

that security and stability is just one input to their decision-making. Next slide.

The current work parties that we have are on name collision analysis. We had a cross-community working session on that, and that will be covered in detail. We have a team working on our organizational review with our independent examiner, we have a work party on WHOIS rate limiting, Internet of Things, and of course our ongoing work parties to manage and run DNSSEC workshops, and our membership committee. We've got a list of recent publications which we'll cover as part of the presentation. And I'll hand back now to you, Rod.

ROD RASMUSSEN: Thank you, Julie. And I do see that I neglected to skip the first agenda item on our schedule here which is to introduce the SSAC members, but we're going to skip that right now. Everybody sitting at this table is an SSAC member, so remember who they are. Wave, everybody. There we go. So remember who they are but hold on for questions later. If we have time, we'll introduce ourselves at the end if there's nothing else to do.

Julie already covered this a little bit, but we do have these open work parties. I'll note that a couple of these will be digging deep on the name collisions analysis project, and other ones are fairly straightforward as to what's going on.

What's more interesting potentially to take a look at is what areas of interest for new work that we may be doing. As a volunteer organization, we have a certain amount of capability to be able to do work on various topics. We do have a lot of members, but they all have different capabilities and expertise that they bring to the table, so we can work on many different things, but only so many things at once, particularly when we have staff resource constraints as well.

So these are some of the things we're looking at, and there are various things around signing a root and what didn't even make it on this list – this list was prepared before the ICANN meeting here – was looking at the KSK roll as well. So actually, if you're wondering where that was, pretend it's the bottom point on the slide there. That is something that we may very well be looking at.

So these are all things that are on the list of possible topics for us to be taking on. We like to get input from the public – the community, obviously, and the board, etc. on areas of interest that are important to the community. So those are some things to keep in mind.

I'll call out a couple of things here. One of the things we've done is gone through all of our past publications and decided whether they're still valid or not, need an update, etc., and are looking to

group some of those together for some updates. We have been at this since 2002, so some of these are a little long in the tooth. And we're also looking to provide our SSAC skill survey, the thing that we use for determining membership, on making that publicly available so that people understand what he qualifications are that we're looking for in SSAC members. We get that question a lot and we're looking to make that – be a bit more transparent about that.

So some things that we've done recently, we're going to actually be covering these in some more depth, so this is kind of just a list overall and the current work we've currently got open which was already being covered. But that kind of gives you an idea of how much we're working on at one time. I'm going to hand this over to Lyman to talk about our current review.

LYMAN CHAPIN: Thank you, Rod. The ICANN bylaws call for a periodic organizational review of each of ICANN's constituent bodies, the Advisory Committees and Supporting Organizations. And our turn has come around this year. We were last reviewed over five years ago. Ordinarily, they tried to do this on a roughly five-year cycle. It frequently takes a little bit longer than that, but our last review I think was in 2009.

We had sort of advance notice that this was about to happen, so going all the way back to July, we formed a work party to oversee our participation in the review. The independent examiner – it took a while to appoint an independent examiner, so although we completed some preliminary work starting in July, including a self-assessment and a survey of our membership, the real work has only just recently begun.

The analysis group was selected to be the independent examiner for the SSAC review in February, and so between now at this meeting when a lot of interviews are taking place and in May, the Analysis Group team is going to conduct their review, do interviews and surveys, document analysis and so forth, and then in June, they'll publish their assessment report.

And just as a reminder, starting with the NomCom review which is also still in process, ICANN is conducting these reviews in two distinct phases. The first phase being a Findings Phase where the independent examiner gathers information and presents a preliminary report that contains only findings. No recommendations, no suggestions for how to change things, but simply what they found.

And then the second phase is a Recommendations Phase. So we'll see the assessment report for SSAC in June of 2018 and then the independent examiner will go off and by November will

produce a final report with recommendations. There are two opportunities for public involvement in this process. the first comes after the publication of the assessment report. There is a public consultation. Not a formal public comment period, but a public consultation when there's a published assessment report available for review and people are invited to submit comments, either individually or as part of other constituent bodies. And then there's another opportunity after publication of the draft final report which contains recommendations for people to contribute to a formal ICANN public comment process. Thanks.

ROD RASMUSSEN: Thank you, Lyman. So at this point, I'm going to be pausing for questions on the first part of what we've done, but I'm going to back it up here to remind folks of two things. One – sorry to go back through all this, but I didn't think about this as we were doing this from a presentation mode – that I'm going to be talking about the names collision analysis project, the evolution of RDS, so anything RDS-related, and then a recent publications. So I don't want to take any questions on those topics at this point. What I would like to get any questions that people have is the overall structure of SSAC, if you have questions about that, and then the topics of interest and a reminder of the KSK roll as well. So we have a few minutes now for anybody who wants to

come to the mic for questions and then we'll move on to talk about the NCAP work party. Thanks.

No questions? Okay, then we will move on to the next section. Think about questions though, this is important. We want to get feedback. Okay, so let's talk about the NCAP, and I'm going to hand it over to Jim Galvin for that. Jim?

JIM GALVIN: Thank you, Rod. So it began in the last ICANN meeting in Abu Dhabi when the ICANN Board passed a number of resolutions asking SSAC to conduct a thorough and inclusive study of name collisions. One of the interesting things of course that pops up right away is defining what exactly a name collision is. And if you take a careful look at the board resolution, you'll see that that's actually one of the first questions that they asked us to do.

Certainly, SSAC has spoken on this before, but I think that we've learned a lot since that point in time. So we have here – what the board is looking for in the large is this is a quick summary of the board resolution as a whole is asking for us to determine whether an undelegated string when the new next round of new gTLDs should come along, whether or not that string should be put into a category of something called collision string. And then of course providing some guidance to the board and the community in making decision about whether or not that string

can be delegated. Perhaps even if it is a collision string, there might be opportunities for mitigation. And of course, once you're on the list of collision strings, are there circumstances under which you could be removed from that? So the canonical issue that we're dealing with today of course is .corp, .home and .mail, so we're going to speak to that issue directly and also create general guidelines and guidance for the board. Next slide.

So an important question here is, why is this an issue and why is the board addressing this? As I started to say, .corp, .home and .mail of course are sort of the example of the day, and I think that most people are familiar with what happened there. You can certainly go back and look at the board resolution for more detailed background information, but those were three strings in particular that the board had deferred indefinitely at the time, and now they're looking to not be in that situation again.

The important thing is that the effect of name collisions on interoperability and resilience is not really fully understood. We have a picture of what that was with the Jazz report in particular, and that study that was done after the next round started, but a lot has happened since then and we certainly have a lot more data that we can work with. So the goal here is to study what we can, find the data that we can and ask questions about that data, and really examine the long-term

consequences and really fully understand this problem space within the context of the new gTLD program and the next round.

So what exactly are we doing? We had proposed a project plan which we talked about and described at length during the cross-community session that was held on Monday afternoon. We got a lot of interactions with the community and we want to thank you for that. We also had a work party meeting on Tuesday morning during which we discussed further details of that presentation.

I think the important thing about this project is it is the largest project of this type that SSAC has taken on, and it's also a new opportunity for SSAC. We're going to conduct this project as requested by the board in as open and transparent a way as possible. So it is going to be an SSAC work party, but we are looking for ways in which we can conduct this work with the community and engage with the community and get input, have the community to have a point of view and an opportunity to examine the work that we're doing.

So the ways in which we're going to do that of course are – an example was this week when we had a cross-community session and we also had an open work party meeting in which people were invited to come and talk and interact with us, and we're going to continue with that process. That's the way in which

we'll conduct this project going forward. We will have opportunities like that that we will set aside.

We're also going to conduct three studies, and in those studies, we are looking to really gather all the data that we can get and actually study that data. In Study 2 in particular, we're going to be looking for root cause analysis and impact analysis of what has happened and what we know about name collisions, and that full problem space. And in the last study, in Study 3, we'll be looking to examine mitigation options. That was also one of the requests from the board.

Right now in the last round, all the new gTLDs were subjected to a 90-day controlled interruption period, and that's what was decided as a way to address some of the name collision issues as we understood them at that time. So we'll be looking to consider if there are other options, better options, or what kinds of things, what kinds of guidelines can be applied to evaluating future mitigation suggestions.

And finally, in general, we want to have a call for participation from the community. We did that this week, and in the future and going forward, we really do want to have further engagement with the community. We very much appreciated the several folks who did come on Tuesday morning and spent three and a half hours with us in our open work party meeting.

We had a very vibrant and engaging discussion, and we appreciate the folks who joined us at that time.

In addition, we will set aside a discussion group that will have – it's a mailing list that will be open for anyone to join. Anyone who is interested in this topic and project will have an opportunity to join that list, participate, offer their own advice, comments about the work that's going on, and bring any particular issues that they want to to the attention of the work party for consideration in the final report.

And our expectation is that we'll have cross-community sessions and open work party meetings at most ICANN meetings so that there'll be ample opportunity for face time also with work party members.

One final thing that we're going to do is for all of our work products that come out of this particular project, we will make them available as a public comment period, adopting the typical ICANN model that we have used for all of the work products like [inaudible] PDP groups.

Okay. And each of the individual studies, we expect to have some summary draft comments about each of the studies and what we're dealing with with them, what we learned from them, and make that visible to the community so that the community

can be interacting with us in a relatively formal way to help us as we move this project along. And I think that's it, right? Yes.

ROD RASMUSSEN: Okay. We'll take some questions on that. And Jim, if there are questions, I'll let you lead the answers for that. Do we have any questions on the NCAP? Comments, any – we have been talking about it quite a bit here, so I'm sure some of you are tired of hearing about it. Going once, twice. Okay, sold.

Alright, so let's talk about something that's related to a word or acronym we're not allowed to pronounce in SSAC because it's all policy-related but, is near and dear to our hearts at the ICANN meeting today. So things dealing with registration directory services, impact and implications of some of the things that are going on in the greater world today, and some of the areas where we believe that the SSAC may be able to have – oops, that's the wrong button. That's not going to do it. That's going to do it. There we go – may be able to provide some assistance to the community, answer some questions, provide some input, etc. in areas that are within our remit.

And these – we've identified three, and there may be more. We'd love to get feedback on that. But we've identified three that may be of interest for us to do some work on. Those are, as you could see, technical abuse of the Internet and being able to deal with

things like large scale DDoS attacks, phishing attacks, botnet command and control, all these things where you have some sort of impact on the operational security and technical communities and being able to deal with these things that various likely changes to access to this data may impact.

Also, law enforcement in a similar vein but for slightly different reasons, but again, dealing with very important issues of abuse and then of the systems itself, and then of course the work they do to utilize resources that they have access to today in order to pursue their investigations.

And then an area of more of a technical perspective is looking at gated access, credentialing and the various things that you would do in some of the proposed regimes around getting access to RDS-type data. These are problems that are solved in the real world and the Internet world – mainly the Internet world – through a variety of methods that are fairly well established and support extremely large infrastructures today. And we have some expertise around that within our membership.

So those are the areas that we have identified, and I figured we could take a few minutes to – if people have questions or input on this particular area. And if you do, please come to the mic. I see some interest on this one. That's good.

IRANGA KAHANGAMA: Hi. How is everyone doing? My name is Iranga Kahangama with the FBI in the United States. I want to say thanks for bringing up this opportunity. I think it's a really good idea, and as a member of the Public Safety Working Group as well, something we'd be really interested to see.

Specifically related to your first point, I think it would be interesting to also highlight and see what the potential could be for the technical abuse in the short term, should we find ourselves in a scenario where access is limited the day after May and that we have a severely limited set of resources for investigations based on WHOIS.

I also want to reiterate that law enforcement access while also very important to us, law enforcement does highly rely on third-party tools and we do use those resources. So I understand that they need to be separated, but at the end of the day, practically speaking, they are very complementary to each other and something that law enforcement would definitely appreciate a little bit more analysis on.

And in terms of gated access, I would also encourage and I would encourage the SSAC to do this type of work. I think it would be really interesting, and I think that as we see some of these models come out, whether it's for third-party access – I know that the BC and IPC just put a model up on their site, I

know that the GAC is going to work through whatever it needs to do, but I think having a little bit more guidance on what would be a framework to do that in a secure fashion would be appreciated and welcomed by a number of our members.

And I think we have a little bit more members of the PSWG here, but unfortunately, they are stuck in the GAC room doing the GAC communiqué. But overall, I really commend this work and I'd really like to see more on this. So thanks.

ROD RASMUSSEN: Before you walk away, a question back to you or just a point and a question. Before the PSWG was created, SSAC was an area where there was a lot of interface and interaction. There's been interest amongst our members to rekindle that relationship to some extent, and I'd like you to take that back to the PSWG as well. And I know somebody may have said something to me last night about that too from the PSWG side.

My question to you is if we were to take on some of this work, would there be some ability for the PSWG to supply some outside expertise into this? While we do have a couple of ex law enforcement folks on our panel, we don't have anybody who's currently a law enforcement officer. And you don't have to answer it right now, but just a thought.

IRANGA KAHANGAMA: No, I think it's worthwhile. I think it's something given the level of interest, especially from our superiors in seeing the WHOIS being maintained as much as they could. Should some real relevant work come up, then that would be something we'd be interested in trying to provide bodies for. And then to your first comment too, that's a good reminder. I don't know if you checked the transcripts from our PSWG update to the wider GAC. We did specifically mention greater interactions with SSAC as one of our kind of mid- to long-term goals and trying to establish a little bit more regular cadence of reporting back and forth would be really nice and something that we kind of on the sidelines discussed maybe setting up for future meetings, but kind of as you said, rekindling that relationship is something that we'd be happy to explore.

ROD RASMUSSEN: And Benedict, you had a quick comment.

BENEDICT ADDIS: Hi, Iranga, does the PSWG endorse a particular model for the RDS?

IRANGA KAHANGAMA: No. We're under the GAC, and so whatever we're doing is going to be what the GAC endorses. You can get me in hot water otherwise.

MASON COLE: Hi, everybody. My name is Mason Cole with Perkins Coie. I was going to make a bit of a speech here about access to registration data, but I see that actually, the SSAC is already going down the road that I was preparing to go down. But I'll just point out that I think the danger that's starting to arise is that starting May 25th, law enforcement, security experts, cybersecurity experts and others who either detect or prevent online abuse or crimes are going to have a very hard time carrying out their duties.

And it's imperative on ICANN to implement a system where tiered access is available to law enforcement and others who are dedicated to doing something about online abuse. I want to call your attention to a potential model for access that was posted by the Business Constituency and the Intellectual Property Constituency. I'd be glad to share, Rod, the link to that. It's on the BC website. But if not that model, it's at least a starting point for the conversation.

And there's an opportunity for SSAC – as I see on your third point there – to deliver to the board some advice that would hasten that process so that when May 25th rolls around, all doesn't go

dark and people who are trying to do their jobs preventing online abuse don't have their hands tied. So I'll take the action step to forward that to the SSAC, and if there are questions that the SSAC has about what that might involve, I know the BC and the IPC would welcome those. Alright, thank you.

ROD RASMUSSEN: Thank you, Mason.

TIMOTHY CHEN: Timothy Chen with DomainTools. This is my first SSAC meeting, so fairly uninformed about the remit, so I apologize. I'll try to –

ROD RASMUSSEN: Welcome.

TIMOTHY CHEN: Thank you. Keep it technical and not policy. Two maybe specific things in being somewhat up to speed on these issues around RDS that I would encourage the SSAC to become involved in if it's within your remit to do so. So building on Mason's point, what this first submitted accreditation model talks about is it hopes that the SSAC can get involved in helping the community understand how to accredit individuals who do the kinds of services that Mason just talked about.

In what has been submitted so far, all I've seen is a callout to the GAC to create lists of law enforcement personnel for that segment and then kind of talking to the concept of barred attorneys for IP-related interests. So that makes sense because there's a clear credential for those two constituents.

In my understanding, in security there's a broad range of professionals that spend part- or full-time trying to defend networks and nation states and everything in-between from bad things. And I'm not clear if there is a unique credentialing body or how you do that, and I don't think a lot of people are, because the security community tends not to be terribly well-organized, especially around things like policy. And so if the SSAC can get involved and help the community figure out this is a very specific way that you could qualify someone in or qualify someone out.

The conversation will rapidly get to that. Having been through these before, it's fairly easy to poke holes in theories that allow too many people through without he right credentials, and so getting very specific about that is extremely helpful, and I think perhaps you're informed enough to assist in that. So I encourage you to do so. That was point number one.

The second point is on what's been called bulk access, which is a difficult term to define for a lot of people. But as many of you know, the security use cases for WHOIS data are many, but some

of the more important ones – and we know this from our experience working with our data – involved being able to look across WHOIS data in the entire purview of DNS.

Whether or not remains as something that we can do I think is very much in questions. We do know that the model doesn't talk at all about what happens once you're accredited behind the gate. If the baseline assumption is a human being can go to a website, break a captcha and get one record and then perhaps go do it again after they submitted their purpose, that's not going to help a lot of the security use cases, and so I hope that we can continue to talk about whether or not there is a solution beyond just law enforcement, for accredited security professionals to get access to this dataset behind the gate at a level that allows them to do at least some of the very important use cases that they have been able to enjoy in the past. And I think the SSAC can play a role in making sure that that conversation happens accurately and with the right context from security professionals instead of just from organizations like us that represent them. Thank you.

ROD RASMUSSEN: Thank you, Tim. My note/comment to one of your comments is that a lot of the security people who care about policy are sitting at this table. There's not a whole lot more. Benedict has a point.

BENEDICT ADDIS: Sorry, this wasn't intended to be a reverse grilling, Tim. DomainTools' business model is predicated not just on access to WHOIS records but historical records as well. Do you seek to have who was recognized in an ICANN context?

TIMOTHY CHEN: Yes. I think it's something that needs to be discussed to understand what the law says about the ability to process historical data after a certain point of usefulness, but we're not talking about policy here. But yes, we have 20 years of WHOIS records in our database, and we're entirely unclear about our ability to use those for the purposes they've been used in the past.

I don't want to avoid that issue. It's such a complex topic right now with GDPR and WHOIS, introducing more –

ROD RASMUSSEN: You said the word.

TIMOTHY CHEN: Yes. Sorry. Just makes it more complicated. I'd rather solve very important things that are in the next 60 days important, as you've heard from previous speakers here, and then get to those

things. So I'd like to have an open conversation about it. we don't want to be seen as an organization – I don't want to be seen as the only organization that has this data, because we are absolutely not, but we are very happy to be kind of the poster child for that if that's necessary. But we want to be seen as an organization that's very willing to have a transparent conversation about how we do what we do, why it's important, the data we have and what we're allowed to do with it, because we want to be a law-abiding organization hopefully still providing services that we know are incredibly valuable to very important people on protecting networks worldwide going forward. The only way to do that is to be part of the solution, and we are always happy to answer questions from anyone here or in the community about that at any time.

ROD RASMUSSEN: Okay. Thank you, Tim. And we're going to – do you have something to say there, John? We need to be quick [now that we're running out of time].

JOHN LEVINE: I can try and be quick. Like many people here, I wear more than one hat. I am the liaison for M3AAWG. M3AAWG recently filed a comment suggesting a specific model for accrediting security professionals by basically membership in the appropriate

organizations. You might take a look at that, and if you agree with it, send in a note saying you agree with it.

TIMOTHY CHEN: It's a great –

JOHN LEVINE: Sorry. Yes. I'm here. I'm John Levine.

TIMOTHY CHEN: It's a great model and I made a note of it on the Monday session on the panel on the acronym, and I encourage more people to read it. It's public on the ICANN website. It was submitted I think on March 8th under M3AAWG.

ROD RASMUSSEN: Alright. We actually had a lot of extra time because nobody asked, [answered] question [inaudible]. I'm going to cut the queue off at the last gentleman there. [Inaudible] That was good. But if you could make your questions fairly brief, I would appreciate it.

CHRIS LEWIS-EVANS: Good afternoon. Chris Lewis-Evans from the National Crime Agency in the UK, and a member of the PSWG. I just want to

support everything that Iranga said. You know, fighting crime is very much a community effort, so it's not just about access to law enforcement, it's access to many of the people around the table and behind me here. So any comments that you can add to help with the accreditation of that community helping fight crime would be really good.

The other ask I think for you is around our registration or accreditation. Obviously, we need to have our queries to be obfuscated or as anonymous as possible to stop bad actors taking action before we can actually do anything about it. So if you could have any comments towards that process on the accreditation models, that would be really good. And finally, do you have a view on the ongoing policy on the new RDS system and whether that should be scrapped and started again?

ROD RASMUSSEN: So there is an older SAC document which is the blaming the elephant one which gets to that. I think in general, looking at things like the technical side of it, using RDAP instead of the current model and things like that, we're absolutely in agreement that we need to be doing that as soon as possible. Other aspects of blow up the model and do something new or different things beyond what we've already [inaudible] we'd probably touch in any future work we did on this topic.

But individual SSAC members probably have the attitude that, yes, we should be doing something akin to what's been proposed by the EWG or something like that in various flavors. I'm not going to commit to any particular one, but there's a sentiment there. Patrik?

PATRIK FALTSTROM: Rod just mentioned SAC 55.

CHRIS LEWIS-EVANS: 55. Thank you.

ROD RASMUSSEN: Patrik bails me out because he knows all these things and I'm still trying to memorize them all.

MARK SVANCAREK: Mark from Microsoft. In a lot of the models that are being talked about right now, there's this idea of anonymized e-mail. It's not really defined right now, but everything that I've seen so far makes it look like it would make the e-mail addresses useless for the purposes of reverse WHOIS, and it occurs to me that you could probably take the contact information in and hash it or something like that to create some other globally unique identifier that could then be used for pattern matching, which

would have less of a feeling of being PII. I haven't come up with any great ideas because you think, “Okay, I'll hash this and everybody has to use the same hash, so there's a dictionary so then I'll salt it but that has to be...”

Anyway, I think it would be interesting to see if there was some sort of a globally unique identifier system that could be derived from something like the e-mail address that would give you the same pattern matching without having the same privacy concerns.

ROD RASMUSSEN: Thank you. Barry, you wanted to make a comment on that?

BARRY LEIBA: I'm not a lawyer, I'm not a specialist on GDPR –

ROD RASMUSSEN: You can't say it.

BARRY LEIBA: From my understanding –

ROD RASMUSSEN: You’re buying drinks at the bar.

BARRY LEIBA: Any sort of identifier that can relate a number of things – can aggregate a number of accesses would still be considered PII even if it were not traceable to the specific individual.

UNIDENTIFIED MALE: [inaudible] privacy-adjacent identifiers.

VIKTOR DUKHOVNI: I'm concerned that any sort of accreditation system will lock out too many individuals. If I'm a postmaster of a small domain, mom and pop business or a small company or even an individual domain, I occasionally need to reach the technical contacts of parties in the Internet that I communicate with – or fail to communicate with more often – to let them know of some concern or interoperability issue. And I don't see feasible to include everybody you need to include and yet exclude everybody you want to exclude in any sort of accreditation system. Is this thing really viable? Who's in, who's out?

ROD RASMUSSEN: Good questions. Greg, how about you? Would you like to respond to that particular one?

GREG AARON: Your use case is a very common one, and contactability is important. The Calzoni model does not take your use case into consideration because you're an occasional user or not a heavy user, and there is no way to accredit individuals. So at the moment, the Calzoni is out.

UNIDENTIFIED MALE: Right. I mean I run a survey of DANE deployment and when I find people mess up, out of the goodness of my heart, I look them up on WHOIS and notify them. So I use WHOIS about five times a day or something. I get locked out.

ROD RASMUSSEN: Thank you for your comments. Thank you all for all your comments there, that was really useful to hear. And yes, there are some issues that we have been discussing both internal to SSAC and our roles in various other efforts within the ICANN community. Let's move on to cover some of the things we actually published. What have we said? And the next couple of slides – actually, the next slide, Julie is going to handle here. Julie?

JULIE HAMMER: Thanks, Rod. Well, at the beginning of this year, the first thing we did was publish a document to tell the ICANN community about

a new document numbering system. To date, we've only had SAC reports which cover primarily technical reports, advisories and comments. But we found increasingly that we have a number of correspondence-type documents that we either weren't numbering or making official in any way to make it easy for us to track, and in fact easy for the community to see what we're saying.

So we decided that we needed a correspondence series separate to the SAC series of reports so that we didn't start, if you like, polluting that document series with a whole lot of more administrative and community-type topics. So the first one was saying, "This is what we're doing and here's our new document series."

The second one in that series was to respond to a community call for input on the final report of one of the CCWG accountability subgroups, the diversity subgroup, and in that report we simply advised that we supported the recommendations of the report, but on the specific topic that they sought feedback on, that is on whether there should be a dedicated office of diversity, we said that we were not convinced of the necessity of that because we were concerned about resource implications. So that was the first two of our publications in that series, and I'll hand back to Rod to cover further information.

ROD RASMUSSEN: Okay. So we're taking advantage of our new numbering system quite heavily already. I think we're up to five or six on this. And that actually reflects a little bit just the nature of ICANN changing our role as an AC which has some interesting implications, but if people have questions about that, we can take those in a little bit.

What this one, number three, was about was we provided some feedback on the review of the NomCom. And in that, we have several kind of findings and recommendations. The overarching theme that we want to make sure people understand that from SSAC's point of view, the NomCom should be making sure that the ICANN Board and other parts of ICANN where it's involved in selecting its members has the appropriate technical background and expertise in order to ask us good questions and be able to deal with the advice we give them.

And given some recent retirements and things like that of people with that kind of background, we feel it's important that the process in general recognizes that ICANN is largely a technical coordinator, so there should be some technical capability there.

And there were various findings and recommendations there, mostly around just how the process works from year to year and some thoughts about making that more being driven by the full

community and being more consistent and more transparent in the spirit of the new ICANN, as it were, and so also that people who may be interested in becoming nominated via the NomCom understand the various qualities that are needed and are being sought out. So that's what we covered there.

Those are the correspondence documents. We also have another publication here which Patrik will talk about.

PATRIK FALTSTROM: Thank you very much. So Document #99 is a response to a question that we got from the ICANN Internationalized Domain Name Guidelines Working Group, and one can say that we are agreeing with the proposal from the working group, we clarified a little bit and said that based on RFC761 which included the conservatism principle, and SAC #84 which describes – our interpretation on the conservatism principle.

Based on those two, we are agreeing with the working group saying that it is very important that the codepoints that are chosen is within what is valid according to IDNA 2008. We're also clarifying a little bit what is meant with both infrastructure records which includes for example underscore and SRV records. We're also clarifying a little bit what's happening at zone cuts where you might have non-authoritative records above the zone cut that is valid according to the child zone's policy but not

according to the parent zone that is a typical situation which we agree that it might be the case that you must allow these situations. But 99 is that we say that we agree with the work party. And then I think it's me again.

ROD RASMUSSEN: Yes, please.

PATRIK FALTSTROM: #100 is a little bit more complicated, so let's spend a little bit more time on that. We got a question from the policy development process working group on new gTLD subsequent procedures, and we got three different questions where. I'll read the first question. Whether the limitations on delegations per annum – 1000 per year – could be revisited given the results of the continuous data-driven analysis of root stability – CDAR – study, and if so, what guidance can the SSAC provide the maintain the security and stability of the root?

The SSAC response based on SAC 42, 46, reports on the root scaling in both root scaling study team report, the TNO's root scaling study, ICANN's summary report and also the CDAR study. What we are saying from SSAC is that ICANN should continue to develop the monitoring and early warning capability with respect to the root zone scaling. We also say that ICANN should

focus on the rate of change for the root zone, and this is something SSAC has said numerous times. We should not look at the number, we should look at the rate of change.

Then we say also that ICANN must structure its obligation to the new gTLD registries so that it can delay the addition of the root zone in the case of DNS service instabilities, which of course is the combination of the two first recommendations. And the fourth and last recommendation is that ICANN should investigate and catalog the long-term obligations of maintaining a larger root zone.

So in the process of developing of interaction that SSAC have had with the subsequent procedures working group, we have over time – when we got more refined questions, we have given more refined responses, but so far, we are repeating what we have said before, so there's nothing new here. Thank you.

ROD RASMUSSEN: Thank you, Patrik. And that brings us to the end of our prepared slides. At this point, we'd be happy to take questions on any of the publications we just covered. If you have any questions about any of those in particular, we'd be happy to take those. And then any other questions and topics that you'd like to bring up at this point that we haven't covered. So if you all run up to

the mic, we can work through the queue. Anybody going to run up to them? There we go, we got somebody.

CHRIS LEWIS-EVANS: Sorry, Rod, can you go back to the slides with all your future plans work for me, please? Thanks. So I think one of those at the bottom was something about domain takedown.

ROD RASMUSSEN: I'll get there, keep asking me your question. Oh, there we go.

CHRIS LEWIS-EVANS: Best practices. So are you looking at a technical implementation for domain takedown, or are you just looking at a process?

ROD RASMUSSEN: Benedict, you want to answer that one?

BENEDICT ADDIS: Hey, Chris. We're looking specifically at a condensed problem which is around the large shadow namespace that's taken up by domain generation algorithms. So it's looking up bulk takedown or bulk how to mitigate the effects of long-term management of DGA domains by registries and the problems that that's caused. Because I think honestly, it's all been a little bit dealt with in the

shadows and under court order, and I think there's no reason for us not to be transparent about how that process happens. But I'm very happy to chat with you offline if that would help.

CHRIS LEWIS-EVANS: Brilliant. Thanks for that.

ROD RASMUSSEN: And this has been a topic we've had for – and it's not a comment back, this is just a further explanation. We've had this as a topic area that has been broader, and now we're narrowing down the scope of this to focus on this particular problem space where we feel we may have some advice that hasn't been touched on in other places. Other questions. Okay, well, I'm not letting you leave early, because if you don't answer questions, we'll ask each other questions up here.

I have a question from the – oh, there it is. Oh, yes, we have time. We can actually introduce ourselves. Oh, and Norm is here, so let's get a question from Norm.

NORM RITCHIE: I'm afraid it's going to be kind of the same questions. Back to the takedown request, is that specifically targeted at DGAs? Or why would it not just be best practices in general?

BENEDICT ADDIS: I'm feeling unexpectedly popular. So we feel that Dave Piscitello's paper a few years back – and maybe if somebody could quickly google it for me, I can give you a pointer – dealt with best practice in single or low number domain takedown really well, and I think as we've heard today, bulk scale becomes something different sometimes. So we feel that we wanted to focus it. Also because I'm pretty scatty, so it felt that it's probably a good idea to focus this early.

NORM RITCHIE: Okay. I wasn't aware that there was an existing one already. Do you have a pointer to there anywhere? Just generally, not specifically.

ROD RASMUSSEN: There was a paper that Dave Piscitello put out a while ago. This is dealing with – and Dave Piscitello, for those of the rest of our audience, he's on the ICANN Security Team, and it was focused on takedown procedures around the appropriate level, developing court orders and the like. We can find that and get that to you.

NORM RITCHIE: Okay. Thanks.

ROD RASMUSSEN: But ask Dave. You have his e-mail.

BENEDICT ADDIS: I have a reference. Thank you. It's called guidance for preparing domain name orders, seizures and takedowns, and that's published as a PDF on ICANN's website. So as usual, use the ICANN search tool, Google, to find that.

ROD RASMUSSEN: There is a whole initiative to replace that search engine. For ICANN, that is. Okay, so since we have a few minutes and no questions, let's just go around the table so that everybody knows everybody's name who was up here. Jay, we're going to start with you.

JAY DALEY: Hi. My name is Jay Daley.

MERIKE KAEO: I'm Merike Kaeo.

JOHN LEVINE: I'm still John Levine.

TARA WHALEN: Tara Whalen.

BEN BUTLER: Ben Butler.

CHRIS ROOSENRAAD: Chris Roosenraad.

BARRY LEAIBA: Barry Leiba.

WARREN KUMARI: Warren Kumari.

LYMAN CHAPIN: Lyman Chapin.

RAM MOHAN: Ram Mohan.

ROD RASMUSSEN: Rod Rasmussen.

JULIE HAMMER: Julie Hammer.

PATRIK FALTSTROM: Patrik Faltstrom.

JAMES GALVIN: I want to be Rod Rasmussen again, but I'll be James Galvin.

JEFFREY BEDSER: Jeff Bedser.

GREG AARON: Greg Aaron.

BENEDICT ADDIS: Benedict Addis.

ANDREI KOLESNIKOV: Andrei Kolesnikov.

JOE ABLEY: Joe Abley.

RUSS MUNDY: Russ Mundy.

ROBERT GUERRA: Robert Guerra.

JAAP AKKERHUIS: Jaap Akkerhuis.

CHRISTIAN HASSELMAN: Christian Hasselman.

JACQUES LATOUR: Jacques Latour.

ONDREJ FILIP: And last and least, Ondrej Filip.

ROD RASMUSSEN: So it was kind of like the movie where the credits go up at the end and there's nothing at the beginning. But we do have at the end of the credits a bonus feature. Please.

BETTY FOSTER: My name is Betty Foster. I come from Guadalupe. I'm part of the French Caribbean. I'm inviting you to come to Guadalupe

because I want to talk about diversity. I could speak in English, but I'm not really good at it so I'm not going to take any risk. It's not a question, but I want to thank you because I realize as a fellow that even at the level of university, the question of IPv6, governance of the Internet, all these subjects are not communicated. They're not part of education, they're not part of schooling.

Students need to know more information and therefore they need more support from you, and they need to be able to understand this information. I'm going to go back home with a lot of information so I can share it with different players. I am also president of a cluster of digital economy with a lot of companies, different companies that are developers, that are communication people and artificial intelligence, etc., therefore I have a lot of information to share. Thank you so much to allow the access to other people who are not part of your world. Thank you very much for your information.

ROD RASMUSSEN: Thank you very much.

BARRY LEIBA: I gather that the Fellows program and the NextGen program are doing a great job with bringing people in from underserved parts

of the regions that we meet in. And I discovered the NextGen presentations a few ICANNs ago and have gotten hooked on seeing what young people from the regions are thinking about and doing. But anyway, I encourage you to repeat what you just said to us tomorrow at the public forum, because that's the perfect place to say that.

ROD RASMUSSEN: Let me add too that ICANN itself, the Security Team does a lot of outreach to those areas of the world and to go and build capacity, in particular around the SSR issues that we handle here in SSAC from an advice position. They're actually in the field helping to create capacity out there.

Okay, well, we are perfectly at the end of our time, so thank you for all your questions. It filled in exactly how we planned it. So thank you very much for attending today. And with that, we're adjourned.

[END OF TRANSCRIPTION]