MARRAKECH – At-Large Leadership Wrap Up of ICANN65
Thursday, June 27, 2019 – 08:30 to 10:15 WET
ICANN65 | Marrakech, Morocco

MAUREEN HILYARD: We're going to have to start. I'm really disappointed that there are – I can only see five ALAC members. Don't we have, like, 11?

UNIDENTIFIED MALE: Joanna's here.

MAUREEN HILYARD: All right.

UNIDENTIFIED MALE: One, two, three, four, five.

MAUREEN HILYARD: Okay. One of the first things I wanted to go through were the action items for this week. If you're responsible for anything, we want to get some timeframes because we don't have to go to the next meeting and go through and find that most of them haven't been done yet. So that's going to be Evin's job. Go for it.

EVIN ERDOGDU: Okay, thanks. I'll just read off what's been noted day by day as an action item. On Monday during the At-Large Welcome to ICANN 65 and policy priorities session, we needed that I would forward the spreadsheet of the ICANN 65 talking points sign-up to the CPWG list and travelers list – that was complete – and that At-Large members would sign up for utilizing the talking points during their sessions. That is also complete.

The next session was the ALAC/GAC capacity building focus group. This was a small setting discussing capacity building focus initiatives. Pua Hunter from the GAC was to share a list of interested GAC topics with Joanna and then group, and the ALAC and GAC staff would help set up intercessional webinars going forward. Joanna Kulesza is to send information discussed in an e-mail to Pua about the capacity building sessions in addition to the calendar invites and to also send the At-Large agenda for ICANN 65. I believe this was complete.

I'm to ask Heidi about specific funding for capacity building outside of CROP and ABRs. Pua Hunter is to present to the GAC plenary on the ALAC capacity building sessions. I believe that was complete during the meeting on Wednesday. Joanna and Yrjo are to present to the At-Large community the idea to have an additional half-day before or after the ICANN meetings for GAC/ALAC capacity building. Yrjo suggested that Pua and Joanna mention these meeting takeaways during the joint ALAC/GAC

session on Wednesday in addition to the policy topics of mutual interest. That's also complete.

The next session was At-Large development of the ALAC hot policy topics document. Joanna and Jonathan Zuck were to work with staff to have a final ALAC hot policy topics document by ICANN 66 or ATLAS III. Myself and Silvia are to create a wiki page regarding RALO hot topics and ALAC hot topics, which would be formatted with a table with six columns, one with ALAC and five for the RALOs. Silvia to work with RALO Chairs to bring Joanna and Jonathan on RALO monthly calls to discuss the ALAC hot policy topics over the coming months before ICANN 66.

On Tuesday, we had the At-Large policy workshop on geo-names. Olivier suggested discussing with the GAC the same issue that the ALAC/At-Large face in drawing consensus on certain issues, including geo-names. I was to create a page with Jonathan Zuck to brainstorm special purpose Consolidated Policy Working Group calls with specific agendas on the topic of geo-names going forward, and, during the At-Large capacity building workshop, an introduction to the policy development at ICANN. I will put the presenters resources on the CPWG, ALAC, and At-Large policy advice development pages and coordinate with ICANN Learn as well.

On Wednesday, we had our At-Large universal acceptance kickoff, and we had many AIs from the session. John and I will share the contacts of the UASG presenters with the Social Media Working Group and At-Large RALO leaders. The presenters at that session requested that RALO leaders share the link in the presentation. Heidi and Silvia are to put the UASG ambassadors in each region in touch with the RALO leaders. Silvia is to work with RALO leadership to make the UASG standing agenda item during RALO monthly calls starting after ICANN 65. John requested RALO leaders introduce themselves to the UASG in the room before the end of the meeting. This was complete.

UNIDENTIFIED MALE: [inaudible]

EVIN ERDOGDU: Amrita noted there are potential UASG funds for traveling, outreach, and awareness on the topic. Heidi will communicate this to Cyrus and his team. John will provide an update to the ALAC on the status of the UASG pilot in a few months before ICANN 66. Jonathan and Maureen requested the RALO leaders and ALSes publish a blog on the UASG. I will contact Edmon Chung to follow up on .asia's exiting UA material for us by the At-Large Social Media Working Group. Edmon requested John e-mail a specific e-mail address for resources. Ajay Data, one of the

presenters, will send UASG resources to John. Finally, I will create a RALO AI tracking page for UASG pilots the following week after ICANN 65.

Then we had an At-Large Internet Governance issues and RightsCon update. I will distribute Nigel's presentation on ICANN's sector membership in the ITU to the ALT-Plus. LACRALO will consider in their FY20 outreach and engagement plans for travel to include going to RightsCon, and all ALAC RALOs to consider and collaborate on future RightsCon activities.

On the session on At-Large community interaction and input to the ATRT 3, Joanna and myself were to share a graphic of Justine's ICANN 65 PDP presentation with the ATRT 3. This is complete.

Finally, the At-Large workshop on consumer safeguard issues, John Laprise noted informal ALAC consensus of the ALAC members present in the room, even though it wasn't quorum, that a public cross-community session on DNS abuse in Montreal would be useful, and the ALAC would be open to co-sponsoring it. It was discussed to include the GAC for potential co-sponsorship. Yrjo and Joanna will coordinate with ALAC and GAC co-sponsorship of this potential session.

Then there was a discussion on what is DNS abuse according to the end user. Jamie Hedlund noted the CCT review and DAAR

report provided that data, and that informed would be distributed.

That's all I have noted so far. If there are any updates, please let staff know. Thank you.

MAUREEN HILYARD: Thank you, Evin. I think that what it does show is it's been a busy week, considering it's been a very short week. There's certainly a lot of follow-up to be done.

I thought I saw Cyrus come in … okay.

UNIDENTIFIED MALE: He's over there.

MAUREEN HILYARD: Okay. While we're waiting for him – I know he's hiding because it's a really good topic he's going to be talking about – I just want to first of all welcome Sarah the last day of our meeting. Sarah has arrived and I know there's an important reason. It's lovely to have you here. Of course, Sebastien gave apologies because he's at the ATRT 3 session with the GAC.

I know there's lots of complaints coming in from all directions about the travelers list for ATLAS III. Because Olivier mentioned GDPR, suddenly we had to pull it off at the advice of ICANN Legal.

We're going to put a couple notices on the page and stuff to cover ourselves. So GDPR is having an impact on us already.

Just so that RALO leaders can tell your members that, if you quickly [got] a list of that page, you might be able to notify your members. But I could do that for you. I could send it to you. Heidi promises that it's going to be up today.

HEIDI ULLRICH: For the record, I said I would ask and do my best.

MAUREEN HILYARD: Okay. Welcome, Sarah. We're really very, very interested in hearing about the future new gTLD round that [might be] proposed. Thank you.

CYRUS NAMAZI: Thank you very much. Good morning, everyone. Our gratitude to ALAC leadership and membership for providing this opportunity for us to come to you for this discussion today. I'll make a few brief remarks just to frame the conversation to let you know why we're here, how we got here, what we're hoping to get out of this discussion, and what the overall objective of it is.

Just so you know, back in the earlier part of this calendar year, the ICANN Board asked us to begin looking into the various

components of what's involved in the new gTLD subsequent procedures, including the PDP Working Group – the work that's going on – for whom (the target). Then completion date of the PDP is the end of this calendar year at the moment; the various relevant reviews that are going on, other components of it that are material in essentially beginning the task of planning for implementation of a subsequent round.

So that discussion took place in a few rounds with the ICANN Board, the combination of which as the formulation of a set of assumptions. These assumptions are operationally focused. That's an important distinction to make for this conversation. Once we actually had these assumptions formulated, we aligned it with the ICANN Board.

The next logical step for it was for us to take it to various constituency groups within ICANN to A) share with them where we're at, what our thinking is in terms of planning for the implementation and B) solicit feedback – this is what we're hoping to get from you – to see whether these assumptions actually are aligned with your own thinking. We've done this with two or three other constituency groups in Marrakech. The ones that we didn't have time to do it with will actually conduct a webinar. Our hope is to complete this task by the end of August, update these assumptions based on the feedback that we

receive, share it back with you, and then take it back to the ICANN Board in their September workshop.

A couple of things that I wanted to note before we begin. My colleague, Trang, will walk us through these assumptions. We circulated a brief paper based on the assumptions. Hopefully you've had a chance to look at it. We have a core team within the organization. This is a fairly complex undertaking in terms of the scope and size of the project. It touches basically on all the functions and groups within ICANN org.

We have a core team. Myself and Trang are here. Ash is sitting there. He's the head of our engineering and IT, a major component of this program. Xavier Calvez is there. He's our CFO, of course, with the checkbook and all of that. We have Karen Lentz, who is our policy guru, sitting next to Xavier, and Kristine, of course, to the right of Ash: project management for the previous round of new gTLDs.

I just wanted to make sure that we're not here to debate the merits of having a subsequent round or whether there should be one and when it should be – all of that. Really we'd like this little bit of time we have – I think a total of 30 minutes – be focused on these operationally focused assumptions.

With that, let me turn it over to Trang to walk us through it quickly so that we have ample time, actually, for a discussion. Thank you very much.

TRANG NGUYEN: Thank you, Cyrus, and thank you, Maureen and the rest of the ALAC, for inviting us here this morning. There are a couple points I wanted to emphasize before we start going into the assumptions. Building off of what Cyrus has said, it's important to remember that these are operational planning assumptions. These are not policies. There is a separate policy development group that is currently looking at what, if any, changes are to be made to the policy on the introduction of new gTLDs. So this is not that work. That work is a separate track of work that's being led by the community. These our are operational planning assumptions to be used for our own internal operational activities in order to get ready for the opening of the next application window. So it's very important to remember that.

If I can have the next slide, please. Thank you. We have about 33 assumptions that we have organized into eight categories. This first category has to do with assumptions around the timing of the next round. There are two assumptions here; in particular, that all implementation readiness an operational activities – everything in totality that we need to do in order to support the opening of

another application window – will be done before the opening of the next application window.

The reason that this assumption is important is because, in the 2012 round, when the Applicant Guidebook was approved, it contained many of the implementation work done with the community, but there were also several activities that were done after the approval of the guidebook. This is assumption that all activities relating and needed to support the next application window will be done before it is up.

The second assumption on this slide is that the [conclusion] of the PDP Working Group's work, as well as subsequent Board action related to it, will be completed before any additional application windows will be open. That's an important point. We don't anticipate opening any additional application windows until the PDP is completed.

Next slide, please. This second slide of assumptions has to do with application volume and processing time. On application volume, our assumptions are that the application volume for the next round will be approximately the same as it was last round, which was 2000, and that this volume will decrease over time in future rounds and that there will be no changes to the current 1,000 TLD-per-year maximum delegation rate. This is what's in

the 2012 Applicant Guidebook, and our assumption is that that will not change.

On processing time, our assumptions are that there would be one application window per year that would last one to three months and that prioritization will be used to sequence application processing like it was last round.

Next slide, please. This third set of assumption has to do with policy implementation, specifically that there will be changes to the policy that will be coming out of the Subsequent Procedures PDP Working Group. So, essentially, it's not simply a redo of the 2012 round. We are anticipating changes. Because there are going to be changes, we will have an implementation phase where policy implementation materials will be developed with community input. This implementation process will result in very comprehensive and detailed implementation materials that are anticipated to go beyond the level of detail that was in the 2012 Applicant Guidebook. All of these materials will have been completed prior to the opening of the next application window.

Next slide, please. This fourth set of assumptions has to do with readiness activities, specifically that the operational infrastructure – we talked about policy implementation on the last slide. This is more around the around the operational readiness, which is the systems and peoples and processes that

we need to put in place in order to operate the next round. All of those activities will be completed prior to the opening of the next application window, and they will be done keeping in mind that we are building this operational infrastructure for the long-term introduction of new gTLDs and not simply just for another round.

Next slide, please. We several assumptions around systems and tools. There are two slides on this. On this particular slide on systems and tools the assumptions are that technology investments are planned to be limited to only those capabilities needed to ensure the security, stability, and consistency of application submission, processing, and communications, and that systems and tools would be designed based on a clear understanding of program processes and requirements. In other words, we're not going to be building a system in a vacuum. Some testing will be completed prior to the opening of the next application window. Along the same vein, all systems and tools will be developed prior to the opening of the next application window.

Next slide, please. This is a continuation of the assumptions on systems and tools. Essentially, development of systems and tools will be focused on solving for data-intensive activities and critical program functions. Existing materials and systems and tools will be leveraged as much as possible. All new systems will be developed on one of three principle ICANN platforms, which are

Oracle, Alfresco, or Salesforce. Developing internal knowledge and expertise will be a priority for us. As little as possible will be outsourced.

Next slide, please. This sixth set of assumptions is around operational processes, mainly that well-defined operational processes are critical to the smooth operation of the program and satisfactory applicant experiences. The design documentation, as well as training of staff on these processes, will be completed prior to the opening of the next application window.

The seventh set of assumption has to do with people. Proactive resource planning will be completed in order to adequately staff the program team to meet deadlines. Work staff will be used to perform program management operations and administration. We will outsource critical application functions, such as application evaluation and objection processing. We currently do not have staff to implement policy recommendations once they're completed or prepare for the opening of the next application window. As many of you know, resources for those activities were not allocated in the FY20 budget, and it was not allocated for in the FY19 budget.

Another assumption is that additional staff will be hired on needed skills and experience to support program operations and that we will augment staff with temporary resources as needed to

address peak workload for activities which are not expected to be sustained for at least 24 months.

The last set of assumptions have to do with cost, that the program will continue to operate on a cost-recovery basis, funded from application fees to be collected, and that comprehensive cost planning for program deadlines and operations is critical for accurate reporting and management of costs, and that we will be tracking closely all costs related to the development work for the next round.

That conclude all of the assumptions that we've had, so I'll hand it back to you, Maureen, for Q&A.

MAUREEN HILYARD: Thank you, Trang. I know that that's just been a brief introduction to you, but are there any questions from the floor?

CYRUS NAMAZI: [inaudible]

MAUREEN HILYARD: Can you take that?

CHRISTOPHER WILKINSON: Do we have remote audio?

JOHN LAPRISE: Thank you very much for coming in and presenting. One issue. Many of our thoughts regarding subsequent procedures and a new gTLD round and policy related. I'm going to table those. But one that is not that we have really made a strong point of is that we in At-Large really want to see the CCT and RPM reviews implemented before this goes forward. That's on, I believe, the first page of assumptions when you're talking about things that have to be put into place before a new gTLD round goes into place.

So do you have a timeline for the full implementation of CCT and RPM reviews? Because that's going to be an absolute requirement for At-Large support going forward for a new gTLD round.

TRANG NGUYEN: Thank you, John. I will try to address your question. If anyone else on the team wants to speak up to this, please feel free to do so. I think you're essentially getting at the question of what are the prerequisites to the opening of the next application window. I know this is a question that many parts of the community have raised in the past, ALAC included. The ICANN Board actually had also presented this question to the GNSO Council and the Subsequent Procedures PDP Working group, I want to say, maybe

a little over a year or maybe closer to two years ago. There was no consensus, even with the PDP Working Group or amongst the various parts of the GNSO and community, on what would be the prerequisites to the next round. There were different opinions as to what would serve as prerequisites. Obviously, the CCT is a bylaws-mandated review of the previous round.

So I think that's a great question. I don't think it's a question that was as ICANN org staff can answer. It ultimately is a decision that the Board has to take one it takes into consideration the PDP recommendations coming from the Subsequent Procedures PDP Working Group and any other advice from the rest of the ICANN organization and any other factors.

JOHN LAPRISE: I understand that, but it will have to be definitely reflected in the scope of this because At-Large at present, is not prepared to support – from all the conversations we have, are not prepared to support a new gTLD round before these things are addressed. So unless we have a timeline for that, that's going to set the timeline for the new gTLD round from our perspective.

CYRUS NAMAZI: Thank you, John. We will take that feedback and [do that].

HOLLY RAICHE: I think that is exactly what I was going to say, that, in fact, we've got real concerns. Our bottom line is that there is no rush. I noticed that you in fact don't have the staff to deal with any policy changes, and what is forecast I the CCT is a lot of recommendation to improve the process to make sure that, before there are new names, in fact, a lot of the concerns that we had that were not addressed in the last round …

What I'm seeing here is a railway track. It looks as if your train is ready to go. We're very unhappy that you think it's ready to go because we don't think it's ready to go. Yes, it's a nice schedule, but don't start putting trains on the track until everybody's comfortable with the actual train you've got. Thank you.

CYRUS NAMAZI: Thank you very much, Holly. Your point is well-taken. Just wanted to make sure that it's understood that, from our perspective, for an organization the side of ICANN org, this is a fairly complex undertaking. So even in the best of scenarios, it's a multi-year effort before we can actually open shop and say we're ready to accept applications.

The objective here has been for us to begin the readiness exercise, seeing that the PDP Working Group, at least in their established timeline, has the end of this year as the goal to complete the PDP. But a lot more work and decisions continue to remain and to be

dealt with, going forward until the Board is ready to consider whether to give the mandate to the organization to go ahead or not. We want it to move something to the extent that we can in parallel and, in fact, have this sort of conversation with the different constituencies so that everyone is on the same page so we're beginning to put thoughts around it and begin thinking about how to go about the implementation of it. But it's a multi-year effort at best.

JOHN LAPRISE: Justine?

JUSTINE CHEW: I actually have two questions, but I'll leave the second question aside. The first question has two parts, both pertaining to costs. The first part of my question is you've identified that the program, when it happens and if it happens, is supposed to be on a cost-recovery basis as was meant to be the 2012 round. Obviously, there is going to be expenses coming out of what you're attempting to do now. But because the application hasn't opened, there won't be application fees to fund this. So my question is – I think Xavier is going to answer my question, but I'm going to pose it anyway – what would be the source contemplated for funding this pre-preparation before launch?

The second question, if I also may add, is, if I may say, I think one of the frustrations that has constantly come up in the SubPro Working Group is we do not have clarity as to the costs, the actual costs, involved in the 2012 round. So when we talk about cost recovery, we actually don't know what cost we're trying to recover. But I understand that's in the past, so what I wanted to know is, what is ICANN org doing for the upcoming round differently to what you have done in the past in order to avoid this situation again? Thank you.

XAVIER CALVEZ: Sounds like it's a question for me. Thank you. We had this question from others, and it's a completely logical and natural question. As Cyrus indicated, the preparation of a round before it starts is a long exercise and a complex exercise.

Just to address some of the prior comments, we haven't started planning yet. What you have seen is an initial thinking about what planning would look like down the road, which we haven't started. When Cyrus said there's a core team present here that is working on it, it's a core team that has a full-time job otherwise. We have not put in place resources yet to even start planning on this program. So I just want to make sure everybody understands the readiness.

So there will be a certain amount of costs to incur relative to the preparation activities of the round before the round starts and therefore before the application fees are connected, which is why you're asking the question: how are we going to pay for the costs of preparing this round before we collect the application fees that will ideally reimburse those costs.

The initial thinking about it that has been discussed with the Board is – I will qualify this later – to borrow money from the current estimated leftover of the current program. You know we have a current program. We have collected application fees. There is currently remaining funds that are aimed at covering the legal actions and other risks that we still have on the current program. With that amount of funds, we are hoping that we will not have that many risks and legal costs of the program and, as a result, there would be money left over from that program.

That is the current plan: to use the leftover of those funds as a source of money to fund the expenses but to repay with the future applications fees to be collected on the next round at the time they would to repay the funds borrowed from this current round so that we keep the integrity of the different round from a financial standpoint. That is the current plan.

Now, there are conditions associated with that, which is, is there going to be any remaining fund dependent upon how much

money we need to spend for defense costs – legal and other risks – on the current round? Those are not finished. You know that. there's many ongoing procedures on the existing program pertaining to very few strings left. But those are the "problem children."

So we don't know for sure if there'll be money left, but we are currently assuming that, when we start and when we need to spend money for the preparation, the source of funding would be to borrow money from those current remaining funds.

If I understood your second question about the principle of cost recovery, which really means you need to know how much cost you're going to have to know how much you're going to need to recover, this is of course of the challenge of the exercise that existed last time. You need to set the fee before you actually know how many applications you're going to have and really what the costs will be.

We have, of course, the benefit of the experience of this currently-finishing round to inform the process of developing estimates of future costs. The PDP that is currently being worked on is also helping understanding what changes to the past round there would be in the next round.

So we will use all that inform to try to project as thoroughly and comprehensively as possible what the costs of the next round could be.

You understand that there's a very big unknown, which is the number of applications. I wanted to qualify one thing here. we are making an operational assumption of the 2,000 applications. This is not ICANN projecting, "We're going to receive 2,000 applications." Nobody has a clue. We don't know. But we need to use an operating assumption to start the work at the time that we will. That is the assumption we're making.

So we will need to project, to estimate, to forecast as much as we can the potential costs. I want to emphasize that the costs to cover for risks of the program, while we have experience now about those risks, will remain a very subjective and speculative exercise. So they will be subjective components into the application fee that we will need to set in order to ensure that there is a cost recovery.

If you look at the current program, we collected $362 million of application fees for the 1942 applications that we had. Right now, we are estimating, before knowing how much money we are going to consume in the next weeks, months, and years on the current procedures that are going on, currently we're estimating that we will have spent approximately $300 million out of that

$360 million. We know we're going to have more costs coming about those remaining strings that are in contention. So we're going to spend some of that $60 million that's left between the $360 million and the $360 million.

If you go back twelve years or eleven years when the fees were set, those who did that – maybe some of you together – did a pretty good job, actually, without knowing anything, in trying to set the fee at a level that would not be too high but would nonetheless recover the cost. So I think that we will need to do as good an exercise as we can to use the experience that we have to project the costs in the future without knowing the number of applications and set the fee accordingly.

There are other elements that enter into the setting of the application fee as well: how high a bar it is in order to enter into the program. There's a number of elements, and I'm sure you involved in the PDP Working Group know a lot about it.

I'll stop here. Thank you.

JOHN LAPRISE: Thank you. At present, we have Tijani, Jonathan, Christopher Wilkinson, and Justine in the queue. Unfortunately, we have a responsibility to – SSAC has arrived. They have a 9:15 presentation. So we are going to curtail conversation on this. I

would ask that those people in the queue communicate with Cyrus and Trang directly with your concerns so that we can now invite SSAC up to the table and hear their presentation.

UNIDENTIFIED FEMALE: John?

JOHN LAPRISE: Yeah?

UNIDENTIFIED FEMALE: [inaudible]

JOHN LAPRISE: No, I'm sorry. SSAC is here. We have to take them. My apologies to the queue.

CYRUS NAMAZI: John, just very quickly. If you think it's warranted to continue this discussion in a live format, we'll be happy to set up a webinar to continue it. I think this is an important discussion to have to hear your concerns, to get your feedback, so if you think it's warranted, your time and ours, we'll be more than happy to make ourselves available for you.

JOHN LAPRISE: We'll make that a staff action. Thank you very much, Cyrus.

CYRUS NAMAZI: And thank you for the opportunity to be here. Thank you.

JOHN LAPRISE: All right. If I can invite SSAC up to the table.

MAUREEN HILYARD: Thank you, everyone. If we could just … [inaudible]. We are very pleased of course to welcome the SSAC team today. Nice to say that everyone has come down. [inaudible] good. There are a few topics that we asked SSAC to raise for us today, so I'll just pass it straight on to you then, Rod.

ROD RASMUSSEN: Hello, and good morning, everybody. Hopefully you've made it through mostly unscathed through another long ICANN meeting, our last day. We've been doing a lot. I know there's several issues. I've had three of four people come up and say, "Can I get two minutes? Can I get two minutes?" Hopefully after this I might have two minutes, but I don't even know what my own schedule looks like. So there's a lot of interest in things that are going on, clearly.

We have a few SSAC members that are going to provide some feedback. We'll have them introduce themselves as they do that

on our activities. I don't even remember what the next slide is, but let's go see it.

All right – oh, yeah. Hey, it's the agenda. That's good. We're going to talk about SAC105 – that's the Internet of Things – one we just put out, and then the DoH/DoT work that we're looking at, where NCAP stands. Also, the registration data service query reporting is about the letter we sent into ICANN that several of you picked up on. Then the review. It's not on here, but given that two people asked me about this already as I walked in the room, we are happy to talk about the EPDP and related issues.

Let's go to the next slide. Does anybody in this room need a real review of what SSAC is? Is there anybody unfamiliar?

We're all veterans. Excellent. Let's move on to the next one. The number is 105 now for publications. This is what we do.

Let's move on to the next slide. This is boilerplate. We have to do it, but we do keep the numbers up to date. This is the recent publications since the last meeting, mainly some correspondence series. If you remember our numbering nomenclature, if it's SACXXX (XXX being a number), that's a report. If it's SAC with the year and a number, that's a correspondence. So there have been a few correspondences. A couple of those were pretty run-of-the-mill things, but we're memorializing those. The registration data

service query reporting we'll talk about, and then we'll talk about SAC105.

Next slide, please. This is what we're currently working on in SSAC. These are current open work items where we have standing work parties doing work in SO. NCAP, which is the Name Collisions Analysis Project, which is on the agenda. We'll wait for the [inaudible]. The SSAC organizational review is on the agenda, too. DoH/DoT is an open work party. We had the high-interest topic cross-community session on Tuesday with the ccNSO. I'm sure there's a lot of questions about that. We'll get that on here, too. EPDP is open.

We just – this isn't on the agenda, so I'll give you a little more insight here. Root server system. We're going to do a public comment on RSSA037/038 and the associated documents that come along with that. We have a work party stood up to provide input on that being led by our non-RSSAC members. We have a lot of crossover between them, but we're including them on there. We're trying to put together a good program. We're trying to lead that, though, from the people who actually don't participate in that directly but know what's going on. So you'll see those public comments from us out, probably on the last day they're allowed. You know how that works.

Internally, we're doing a lot of work on how we do our own working processes. We're actually working through an exercise, potentially, on a strategic planning mechanisms akin to what ICANN org itself did much shorter to help align our work in there and our priorities. We hope to share that with you at the next meeting in Montreal. We'll see how that goes. We've sort of kicked that process off, but if that works well, we're going to share that with the rest of the community as perhaps an example of ways to approach some of these things.

We always having emerging security topics and the DNSSEC Workshop and our membership committee. Speaking of the membership committee – I'm going to put a plug in that for [now] because it's not there – we are definitely looking for new members. You've sent us a couple of great members. Andre has been awesome.

UNIDENTIFIED SPEAKERS: Yay!

ROD RASMUSSEN: Yeah, I got it right this time. He gave a really interesting talk yesterday, and I think he's given a lightning talk at every single ICANN meeting that we've had. It's always been on something new and interesting and different. We're continuing in our striving

for diversity around the world, in particular with people with really good, strong technical security backgrounds, so if you know of such people and are interested in helping us understand areas where we may not have coverage today, especially from skills and exposure to different kinds of risk, we highly encourage you to go to the SSAC portion of the ICANN website and take a look at applying for membership. We'd be happy to take on some more folks. So, please, even if it's not you, if you know somebody that fits that bill in your region, encourage them to at least think about it and take a look.

Okay. That shameless plug is over. We'll – oh, this is my water. Good. Then these are some of the things we may be looking at. We're meeting later today with the RSSAC. This got brought up to me by two different Board members: the hyperlocal root, which I don't necessarily want to spend a lot of time talking about here, but it seems to be getting a lot of interest. If there is a lot of interest in that, I'll find somebody who can actually speak to that better than I can in this room.

And the DNSSEC key management stuff. Especially as it comes into a lot of the operational stuff, there's some issues here that have been brought up that we want to potentially take a look at because they would require some policy changes in order to make the technical side of that possible.

We're definitely looking at some of these abuse areas, whether it's takedowns or studying abuse. It says new gTLDs, but actually that's narrower than the focus that we may be doing. And of course, the domain name hijacking attacks that we talked about in Kobe remain a really hot topic because some of the activities continue to this day. So that's likely to jump up the priority list. These are areas that we are thinking about, so if you see this list and you think this is something that the ALAC is interested in supporting us doing, we'd love to get that feedback because one of the things we're trying to do is be as responsive to the community as we can.

Holly?

HOLLY RAICHE: Really brief question. If you're studying abuse in the new gTLDs and right now what we just had a session on was the process for going ahead, it strikes me that I would like to know what you're saying about the abuse before we actually continue with the next round. Do we have advice on that? Thank you.

ROD RASMUSSEN: You're asking about timing on that? Yeah. Okay. So that one is, literally, as I'm looking at my to-do box, the next to kick off. Now, that could get superseded, but we do have available members

that have that background to do that work. So that's something we're … I'm not making a promise that we're going to kick if off right away. Don't take that as a commitment, but it's certainly one that's right at the top of the stack. As I said, that might be a bit broader than just new gTLDs because what are you going to compare it to, right? Anyway, that's the story on that.

Again, think about those that were on the list. Let's bring that up in discussion in a bit. Let's move on to the next slide. I think it's [Nick] –

UNIDENTIFIED SPEAKER: Cristian.

ROD RASMUSSEN: It's Christian that's going to talk about SAC105. I know there's been a lot of interest in the IoT stuff, so I'm going to have Cristian give a couple of highlights and then take your questions. Cristian? And he's over there.

CRISTIAN HESSELMAN: Yeah, I'm all the way down here. Thank you, Rod.

ROD RASMUSSEN: Introduce yourself too, please.

CRISTIAN HESSELMAN: Oh, right. I'm sorry. I'm Cristian Hesselman. I'm with the SSAC. I'm the work party leader of the IoT Work Party. We delivered this report, SAC105, at the beginning of June. The title is The DNS and the Internet of Things: Opportunities, Risks, and Challenges. The report is a different report than what you're, perhaps, usually used to from the SSAC because it doesn't contain any recommendations. Rather, the goal of this document is to facilitate discussion within the larger ICANN community on the interplay between the IoT and DNS ecosystems, which are two, I would say, parallel and co-evolving ecosystems that interact with each other.

What we did in this document is provided a tutorial-style discussion on the interaction between the IoT and the DNS. We started out by basically painting our model of what we think the IoT looks like, which is basically a large number of IoT devices that interact with services to provide their functions. For instance, you could have a sensor in your door lock that sense when somebody is near the door lock and sends that information to the service. The service analyses it and then instructs the door lock to open. That's a very simple example.

The important thing, of course, is that we know that these IoT devices make use of the DNS to locate these services, so we split

– and that's basically the model that we outline in the paper: IoT devices, networking connectivity, and services, and the DNS that enable the IoT devices to locate these services.

Then we continue with basically opportunities and risk. We speak about the opportunities that we think the DNS has for the IoT. This basically stems from the fact that the DNS is a globally-distributed infrastructure that provides various security function that can help in fulfilling the new types of security and stability requirements that come from the IoT because IoT devices interact with people's physical environment. So this means is has an impact potentially on their safety and also on their privacy.

One aspect we discussed there is that we think that DNSSEC, for instance, would be beneficial to IoT devices. For example, if they could validate DNSSEC signatures, then this would reduce the probability that this door lock I just spoke of would connect to a malicious service and send information to that malicious service but also accept malicious instructions from it. So you would basically service the binding between the IoT device and the service that it makes use of. That's just on example we listed. We listed a few more in the paper. So that's opportunities.

Then we go on talking about risks. One of the risks that we discuss is IoT botnets. We all heard about the Mirai botnet back in 2016 that generated a pretty large DDoS attack. We basically studied

the scientific literature to get some numbers on how these IoT botnets currently evolved. So the state of the art is that there are around 400-600K infected devices and that this botnets can grow in size within maybe tens of hours. So they can spread quite quickly. So that's basically on the risk that we talked about.

Then we had a chapter on challenges, which basically ties the opportunities and the risks together. The first challenge that we discussed in that part of the paper is the development of an IoT security library that makes DNS security functions available to IoT software developers. This is important because IoT devices generally come with a very low level of security, which is potentially caused by IoT software developers not being familiar with DNS security or network security at all. So there's an educational component involved there, which we also speak about.

The second that I want to highlight here is basically to address the risk of IoT botnets. We foresee that a whole range of measure need to be taken, ranging from securing the IoT devices themselves, which is, again, coming back to educating the IoT community, perhaps, on how they need to use the DNS and DNS security. So securing IoT devices, but also setting up security services in edge networks so that they can basically clip off DDoS traffic when it comes from infected IoT devices early on. So really close to the source.

Then we also talk about how you could enhance the, let's say, service side by, for instance, enabling DNS operators to exchange information about DDoS attacks. For instance, if a DNS operator gets hit by a DDoS attack from an IoT botnet, it could basically make a description of what this DDoS traffic looks like and then share it with other DNS operators so that they are prepared in case the attack comes there way.

So that's basically what we speak about in the paper: opportunities, risks, and then challenges. And we conclude with that basically we'd like to have a discussion with the larger ICANN community, which is basically also why we're sitting here. Thank you.

ROD RASMUSSEN: Thank you, Cristian. Also I'd like to point out that Cristian has recorded a video, which will be posted shortly, on this. We will be doing some blog posting and trying to – let's keep it at the prior slide, actually. So I've got a question or two here. I just want to put a couple of points here. We're going to be trying to be publicizing this, and we really hope that your members take a look at this. I know there's been a lot of questions about IoT that we've had over the years from you guys in particular, a lot of curiosity there.

The question there: how many people in this room besides SSAC members have read this? If you could raise your hand.

All right. Well, you beat Tech Day.

UNIDENTIFIED FEMALE: Wow.

ROD RASMUSSEN: Yeah. We have three. We had two at Tech Day who were not SSAC members. By the way, I was remiss. SSAC members who are in the room, could you raise your hand?

We've got nine folks and a bunch in the back. Okay. And we're supposed to do that, I think. Anyways, those are various members that were able to be here today. We do have some time after this between now and our next meeting with the RSSAC, so those people who said they want two minutes of my time? You can do that and see other members as well if there's a big queue for me because they an answer the questions probably better than I can. So we want to promote that, so please. There's three. There's a lot more to go.

We want to get from this input for if we need to additional work to help inform the community about various issues. We didn't give any recommendations, per se, in this one. We were trying to

get some of the fud and the confusion that people may have out of it and actually reframe this in the DNS world and the areas that the ICANN org community of the DNS infrastructure live in and separate out all the other stuff that people are working on.

UNIDENTIFIED MALE: Rod, that's really important because there's a whole heap of other documents out there but, as far as I know, this is the first one that really talks about the IoT in combination with the DNS. So that's really the core focus of the document.

ROD RASMUSSEN: Yeah. It took a while to get that scope. We've been talking about this for a while [after] doing this paper, and part of the struggle was scoping it properly so that we made it really focused for this community to be able to do something with and not just repeat a bunch of things that other people have done really good work on. So we referred a lot. There's a lot of references in this document as well. So, for those of you who are interested in more, you can look at the references.

Who had questions?

UNIDENTIFIED FEMALE: [inaudible]

ROD RASMUSSEN: Jonathan?

JONATHAN ZUCK: Thanks. I had an interesting experience once where I went out to dinner with a cattle farmer and he ordered his steak well-done. I just wondered what he know that I didn't at that point. I'm just curious. As a practical matter, since we have so many members of the SSAC here, how many of you are making full use of IoT devices in your homes? That's thermostats, Amazon key ring, doorbells, etc. How many people are feeling confident enough in those technologies that you're using them?

All right. That was my question. Thank you.

ROD RASMUSSEN: Using them because we're confident in them or because that's what we have to do?

JONATHAN ZUCK: Because you're confident in them.

ROD RASMUSSEN: Or maybe we're messing around with them.

JOHN LAPRISE: Javier?

JAVIER RUA-JOVET: Thanks for that paper. This is just out of pure ignorance. Why would IoT devices use … We talk about DNS and IoT. I can easily see IoT devices just talking to each other with IP addresses, just pure numbers. Are we talking about that IoT devices will also have domain names to communicate when we talk about DNS? Or it's just IP addresses communicating amongst each other?

CRISTIAN HESSELMAN: Actually, there's various types of IoT. We described two different models in the paper. I didn't talk about that today. It's basically what we call – I forgot the name, but it's IoT devices directly connected to the Internet. So they have an IP address and the connect to services by using the DNS. This is similar to how traditional laptops and phones and that sort of thing use the Internet.

There's also the model in which IoT devices do not have an IP address. In this case, they can usually connect to a gateway device. So they have maybe a Zigbee protocol or something like that they use to connect to a gateway. Then the gateway connects to the Internet. So you're right. Not every IoT device will have a full IP [stack] because we're only speaking about the

devices in this document that really have an IP stack onboard and use the DNS to locate their services.

But we also know that, from various measurement studies, that quite a few devices do that – things like lightbulbs, sleep trackers, sleep monitors, light switches at home, smart speakers, and that sort of thing.

JOHN LAPRISE: One last quick question for Andrew because I don't see anyone else and I think I'm the list person in the queue. Is there a rationale to have a special class of TLDs that are for IoT only? Are there security advantages or operational advantages to having IoT-only domains?

ROD RASMUSSEN: I actually asked this question myself. I don't remember who I was talking to. I said, "Did anybody even get .iot as a TLD?" At least it's not delegated. I didn't look to see if somebody applied for it or not. Yeah, it's an interesting topic area, and it ties into NCAP a little bit, too, when you think about it, because people do define things, then may use a different protocol, actually, and create a namespace for it.

CRISTIAN HESSELMAN: We did not specifically speak to that particular topic in the paper. What we did talk about is that the security of registrations services might become more important because imagine that there's tens of thousands of IoT devices out there and they all make use of the same domain name. Then the impact of a domain registration hijacked, for example, could be quite severe. So this might also be an opportunity for registrars to provide additional security services for domain names associated with IoT devices rather than with traditional content and services.

ROD RASMUSSEN: Yeah, it certainly touches on other work we're done – SAC040/044 – around registration service protection, etc. We touch on that in the paper. You might want to consider, having a domain name for IoT devices, not letting it expire, for example, because a whole bunch of devices may start sending a lot of queries for a domain that doesn't exist. That has other implications as well.

All right. We might want to move on to the next topic?

UNIDENTIFIED SPEAKERS: [inaudible]

ROD RASMUSSEN: Oh, I'm sorry. Was there another question? Okay, go ahead.

[JAVIER RUA-JOVET]: Just a quick question that comes from the question that Jonathan asked. I have IoTs in my home. Do you know if there exists an application that tells you if your IoT is compromised or not, or do I have to reboot it?

CRISTIAN HESSELMAN: Thank you for that question. That's something that we also talk about in the paper. There are two components there. One is, do you know what information your IoT devices are capturing about you, and with whom they're sharing that for processing? You probably don't. You could imagine that you would want some sort of GUI or something that would make that more transport.

The second one is, how do you monitor in your home or other types of deployment scenario how IoT devices are being compromised? There is various prototype systems at this point where people are looking at how can you protect home networks by installing a separate security hub, either as a device or as a software package that runs on another device.

ROD RASMUSSEN: Okay. We have 15 minutes. I see Olivier has got a quick question.

OLIVIER CREPIN-LEBLOND: Thank you very much. I'm just going to try and be very quick. I noticed you just mentioned IoT devices. Do you differentiate between different types of IoT devices? Because another track that I've followed is consuming IoT device security versus medical IoT devices versus automotive IoT devices, which is another class. They are vastly different. And industrial IoT, of course, is another type. The U.K. government has established some guidelines for IoT security for consumer devices and has steered well-clear of the other ones because it's just a different track. So are you looking at different tracks rather than general? Because they're very different from each other.

CRISTIAN HESSELMAN: This is something that we discuss in the introduction of the paper. We did spot that the difference, and there is also a figure in there that we took from a different paper that gives an overview of the different ranges of IoT devices out there from a consumer perspective.

But you're right. If you do intelligent transport systems in urban areas for example, that will be a completely different scenario. However, these devices may still use services somewhere sitting in a data center. At that point, they will still use the DNS. So we did identify these differences, but we took the horizontal approach, if you will. We disregarded specific verticals and said

that some of the points that we discussed may have some variations within these verticals. But we tried to provide a [generic] discussion.

ROD RASMUSSEN: We're going to move on because we're less than 15 minutes at the moment and I want to make sure we at least touch briefly on the topics. A bunch of the answers to this were "Read the document" because pretty much all the questions are answered in the document. We are going to move on. If we have time at the end, we can come back. As I said, we'll have members hanging around a little bit at the end if you want to ask questions.

DoH/DoT and DNS-over-HTTPS/DNS-over-TLS. Move on to the next slide, please. I didn't pre-position Barry or Susan to come up, so I'll just do this really quick. If there's questions, we can grab somebody to come up if I can't answer it.

We had a session on Tuesday. Hopefully a lot of you were there, where we got together with ccNSO and went over a lot of the issues. We don't have anything to report yet on this. We just fired up the work party. What we're trying to do with the work we're doing is separate out the issues and put them in proper context because there's a lot of uncertainty and a prejudicial, if you will, opinions on DoH and DoT and a lot of things and a lot of lack of knowledge. What we want to try and do is clarify the situations,

separate the hazards, and describe the protocols and how that works and how that provides benefits and may have potential costs and then how they operationally configured, which brings up a different set of issues.

These issues get conflated quite a bit because this came to a lot of people's attention due to a particular set of circumstances, where there's been this assumption about what DoH means and what it's there for. So we're trying to take and separate all these things out and talk about the benefits, the drawbacks, the potential challenges, etc., and present that in a very scientific basis.

There may be some recommendations that come out of that. I guarantee you were are nowhere close to a consensus on what those recommendations will be at this point, so all this work is preliminary.

One of the big things, though, that we want to assure this group and everybody takes away from this is that DoH/DoT, whatever you are looking at from a privacy and encrypted message position, has nothing to do with DNSSEC. They're orthogonal. You have integrity that DNSSEC provides that does not provide encryption and vice versa. And there's a lot of confusion around, well, does DoH/DoT make DNSSEC unnecessary? No, DNSSEC is still necessary for it's job and, and the transport that you put it

over has nothing to do with the job that DNSSEC does that's really important to know up front.

Could you move to the next slide here? I just want to make such I catch any highlights – oh, this is what I just talked about. Could you move to the next slide? All right. We're going to focus on trying to deal with this issue of deployment versus the use of technology. If you were at the presentation, you saw different deployment models. Those were only a few examples of the deployment models. There are many of them. And also try and separate out some of the issues that DoH/DoT have as far as concerns that people have that exist in the non-encrypted DNS world as well because you can use VPNs and have some of the same problems. But people haven't been paying as much attention to that. So those are the things we're going to cover.

Susan or Barry, did I miss anything really badly that I should … okay. I'm not seeing anybody getting upset.

Questions on where we are there with respect to – remember, we are very preliminary.

Holly?

HOLLY RAICHE: Really quickly, we had a presentation in Kobe where two issues were raised. One is that, because you're actually tunneling, you're

tunneling past things like firewalls and things that corporations have put into effect. So, in fact, you're gaining privacy. You may be losing something else.

The other issue raised was that the [inaudible] one to particular resolvers. Now, at the moment, one of the safeguards for resolvers is there are so many of them. But if you start to have favorite resolvers and you have fewer of them, it's easier to target. Those are the two things that were raised in that presentation. Thank you.

ROD RASMUSSEN: Thank you for that. Those are definitely areas that will be covered in the work party. Those are issue we're very well-aware of as areas of contention and trade-off. So that will definitely be covered.

Warren, did you want to add a point? Introduce yourself. We are limited for time.

WARREN KUMARI: Warren Kumari, part of SSAC. So that all depends upon the deployment model. That isn't really part of DoH and DoT itself. It's if applications force you to use a specific set of resolvers using DoH. Hopefully applications will just follow the standard "Use

your existing system resolvers," in which case all of your existing protections apply.

ROD RASMUSSEN: Thank you, Warren. Any other questions before I move on?

UNIDENTIFIED FEMALE: Satish.

ROD RASMUSSEN: Satish?

SATISH BABU: Thank you very much. I have a question on the motivation for providers, like Google or Cloudflare, for providing these services. While it was earlier decentralized – DNS was decentralized – everybody was catering to their own small communities. Today this is being centralized at a very large scale. Why should these people provide these services? What do they get in return? Is it the data?

ROD RASMUSSEN: I'm not going to comment on that particularly right now.

UNIDENTIFIED FEMALE: [inaudible]

ROD RASMUSSEN: I'm sorry?

UNIDENTIFIED FEMALE: [inaudible]

ROD RASMUSSEN: Oh, Tim? Okay, go ahead.

TIM APRIL: Not speaking as one of those providers but having talked with many of them, at least many of the large quads, usually, have a specific policy that they do not collect data. They do not investigate data. They don't share that data with anyone. They're mostly doing it for decreasing latency to make it so that the end users are able to resolve names and get to web pages faster because trying to reduce the time to displaying the web page is key for many of those organizations.

One of the quads – I think it's Quad 9 – tries to market themselves as being there for security reasons, but many of the other nameserver providers are doing for enhanced speed of resolution and reliability.

WARREN KUMARI: Actually, can I respond to that as well? Good, the mic is on. Warren Kumari. As well as SSAC, I work for Google. Google runs 8.8.8.8, and the reason we run that is because it makes things faster, which makes users happier, which means they use the Internet, which means that they click on adds. So this is not entirely a good for the world. Faster Internet means people click on ads.

We do have our privacy policy about that all listed under the Google public DNS thing. Yeah, we don't mine the data. We don't collect. We use it for logging for a really short time, just to make sure the service works, and then we aggregate. It's purely "Click on ads. Make us money."

UNIDENTIFIED SPEAKERS: [inaudible]

ROD RASMUSSEN: Go ahead real quick.

BARRACK OTIENO: Thank you. Barrack Otieno, ALAC liaison to the ccNSO. I have a question regarding standardization. Are you limited to the IETF standards, or are you working also with the ISO information

security management system standards? I would be very curious to hear if you've gone beyond just the IETF standards.

The same question also applies to the previous presentation on IoT devices because at the local level in our countries, normally we are regulated by ISO standards. So how are you working across these standardization areas?

ROD RASMUSSEN: That's a good question. We have, as I said, just kicked off that work party. We actually haven't addressed that part of the scoping, so the fact that you brought that up? We'll talk that about the work party. So I don't have an answer for you today on what the scope will be on that.

UNIDENTIFIED MALE: [inaudible]

ROD RASMUSSEN: Yeah. For IoT, we did take a look at some. Cristian, do you want to give a quick …

CRISTIAN HESSELMAN: Yeah. Our discussion focuses on DNS and DNS-related protocols.

ROD RASMUSSEN: [inaudible]. Basically that's one of the reasons we focused it: you could get into a whole long, larger universe.

Okay, let's move on really quickly to … are we good? Okay. Let's move on. NCAP. Jim, do you want to give just a quick update and introduce yourself as you do?

JIM GALVIN: Sure. Thanks, Rod. Jim Galvin for SSAC. Let me acknowledge by Co-Chair, Jay Daley, who's actually not present here.

Just to keep it short, there's a lot of information on the slide here. Most of this is updates and stuff that you had before.

We can go to the next slide, please. I'll just highlight the stuff which is new. Let me highlight the Study 1 gap analysis. We are now in place where we created the – OCTO is Office of the Chief Technology Officer, which now has the RFP for Study 1. Its release is actually imminent, and we're expecting it actually to come out within a couple of weeks here, shortly after the ICANN meeting, so that this process can now get started. So the NCAP process has been a little bit of fits and starts here in getting going, but we're now in a really good place.

Move to the next slide, please. This has the whole timeline stuff here. We do have a discussion group. It is open for anyone to join as part of being inclusive in the NCAP process. The only

requirement is you have to fill out a statement of interest, the usual kind of GNSO process for creating broad community working groups. If you go to the community wiki area for the NCAP project, you'll find a mechanism for filling out the form to join the discussion group and become an active participant and be engaged, and now would be a good time to do that. It's a rolling, open opportunity for anyone who wants to be involved. You can always be an observer, so the meetings and such are generally open. You can always come and listen and see the archive on the mailing list.

Now that the RFP is imminent for a contractor to begin Study 1, we expect that to come out in July. Best-case scenario, hopefully we'll be able to get a contractor in place in the August to September timeframe. These things are unknown. It just depends on what happens. We hope to get started with some actual work and to have our first face-to-face very productive meeting in ICANN Montreal.

I think that's it, right? I think that's the last slide, isn't it? Yeah.

ROD RASMUSSEN: Okay. In the interest of time, we're going to move on to the next bit because we want to make sure you're aware of the next item. Then we'll have, like, two minutes for anything.

You can move on with the slides, please. I believe that – yeah. There was a letter. I know some ALAC members have seen this and asked about it. Earlier this year, trying to answer a research question about the effect of GDPR on WHOIS queries, some of our members – I'm the one who asked the question, so blame me. But some of our much more deft members at doing things with data pulled the data from the reporting systems that ICANN has around WHOIS queries that all the registries provide statistics for to try to answer that question of how many WHOIS queries there are per day: about seven billion – that's "B," billion. We don't know what they are all the time, but that's what's being reported.

What we found, though, is that the data is being reported inconsistently between the various registries. Digging into the situation, it turns out that people were interpreting the way the contract language specified how to report the data. So, if you were running a backend registry operation for multiple TLDs, for instance, some people were reporting the same number of WHOIS queries for each TLD [inaudible] servers, which obviously isn't very likely to happen in the real world.

We had some discussions with registries to back channel to figure out what was going on and found out that the problem was a little bit more than just one or two registries having a difference. It was a lot of different interpretations. We talked to a couple of parts of ICANN that deal with these things. Then, given the scale of the

problem, we handed this off to ICANN to try and organize a synthesis of view of how to report this stuff.

We had a discussion with the registries here at ICANN 65 that was facilitated by ICANN. From the results of that discussion, we are not going to have consistent data anytime soon in the WHOIS reporting. There's still differences of opinion around how to actually count queries of different types. So there's more work to potentially be done here around defining how to count and what the actual purpose of collecting this data is in the first place because this is a legacy thing. That's where we stand. So this is an area I know tweaked people's interest. I want to make sure this was out there and people had that.

We are right at time. As I said, we are going to be hanging out. I know John's probably not going to let us go over time, are you?

JOHN LAPRISE: It's the Chair's prerogative.

ROD RASMUSSEN: Okay.

MAUREEN HILYARD: Yeah. Five minutes.

ROD RASMUSSEN: Five minutes. We got an extra five minutes. Any questions on this? Other that, I know some of your folks want to talk about the EPDP. So whatever time [inaudible] questions takes out of that.

MAUREEN HILYARD: [inaudible]

ROD RASMUSSEN: Okay. And if any of your members – oh, go ahead.

JONATHAN ZUCK: Sorry. I guess my question is about the names collision project. I guess it was a very procedural report on that, but is there any kind of impressionistic report you can give on how that went? Because we were part of the group that raised the alarm that nobody was attention to the issue when you raised it in 2012. But now the folks that are driving for a new round are scoffing at this issue having been raised like it was Y2K and nothing ever happened and why are we making such a big deal about it.

Do you have some layman's impression of how this issue played out over the last round and whether it's likely to be a serious issue going forward?

ROD RASMUSSEN: Well – you want to go ahead with that, Jim?

JIM GALVIN: Yeah. SSAC has been very clear in its stated position in all of this. Names collisions are a reality. They're going to continue to exist. We believe that the issue does need to be studied and understood, and the community should take that under advisement and do something with that.

I know there's this tension about the scheduling of the next round versus a full understanding of name collision analysis. SSAC's position is that this analysis really should take place. We're not making a commitment as to what the community wants to do about timing of the next round versus name collision analysis. But it is important to fully understand the risks and mitigation opportunities with respect to it. That's been our stated position from the beginning in a variety of different ways. I'm actually forgetting the previous report that had that statement in it.

ROD RASMUSSEN: I'll also note that the [home/corp] mail situation is part of that as well. That needs resolution regardless, but that's outside of the next round. ICANN is committed to spend a fair amount of money already on the first part and potentially more. So, from our perspective, we're going forward with this and trying to make sure the next round does not end up with any issues in it as we

said we should have done in the first round, too. We'll see how all the other politics play out.

I wanted to have a quick discussion around what's going on with the EPDP. We have made our position clearly on some of this. We talked about where we differed on Phase 1. That obviously has to be dealt with. We're concerned about making sure this gets done on a timely basis in Phase 2 and actually had direct conversations with the Chair on that. They're sitting there right now and hopefully making progress. We have been very clear in our position around access to the data for security research purposes.

One of the things we're going to try to do moving forward is get this amorphous term of security research better defined and maybe with some different language. We have incident responders, which are a vastly different thing than somebody doing a research. I think the terminology is getting in the way, it seems, within the EPDP. So that's an area which would be useful for us to potentially collaborate on making sure we're talking properly about the use cases and the types of requests that may be made. Obviously, we made a lot of statements around the universal access model and the need for law enforcement to be able to access the data. Those are [inaudible] SSAC consensus positions. We do have a work party that is working behind the scenes of our reps. If there's interest in having conversations

between that work party and your own work party, I think that would be good. We're doing the same with a couple of the other SOs and ACs.

What I'm finding is that all the different parties that are involved want to talk to us as SSAC and make sure we're aligned with whatever they're doing. We're sticking pretty much to what our remit is, but if nothing else, we can backchannel some of this stuff to each other because there's some groups that just don't trust each other.

JOHN LAPRISE: Thank you, Rod. Yesterday we had some backchannel conversations among ourselves on this very topic. One of the things that arose is potentially the opportunity for a four-party advice to the Board on this issue because all the ACs are capable of issuing advice but this seems like something where we all have common interests in granting security researchers access for stability and security. It's something the ACs could together on and issue a single statement to the Board about this and make it a very strong statement about it. So it's something that we're thinking about and we're interested in.

ROD RASMUSSEN: Let me just respond to that. This came up at the very last minute in Kobe. There was outreach to do a joint statement, which at the time, there's no way for us to go through a process in SSAC that quickly.

If there was something I could take to the membership and we could decide whether or not we wanted to do that, no guarantee at all that would happen because we've never done it before, so it was set a precedent. Amongst security folks, there's caution to do things that are new and different.

But I think, at the very least, it would be worth having a discussion around what mutual interests are on this because I think there is a lot of alignment on these topics and how one might phrase something so that, as in Kobe, we can react to that, if nothing else. At the Kobe meeting, I acknowledged in our meeting with the Board that that kind of information that was aligned exactly with the things we'd already said. So that would be probably the better way to deal with something like that: have something where we can react to it, rather than try to out jointly. But I'd be happy to at least bring it up to the membership.

OLIVIER CREPIN-LEBLOND: Thank you very much. There is indeed precedent in the ALAC, reminding the Board of a specific SSAC advice. I think it was the one on name collision, and it was in Durban. The SSAC had issued

its advice at, I think, a meeting earlier. The Board had ignored it. The ALAC picked up and basically said, "You have to listen to these guys." I'm paraphrasing, obviously.

So I understand the position of SSAC being particularly just focused on technology and on specific SAC advice, so might I suggest to John Laprise that we discuss this afterwards? Maybe we'll just try and see if we can get the other ACs to work together and support the SAC advice that is being provided already.

ROD RASMUSSEN: Yeah. And let me know that that was appreciated at the time, and the GAC has done that on a regular basis. It referred – and that's exactly what I'm talking about. A joint statement is a different beast than saying, "Yes. What those guys said we agree with, too," right?

OLIVIER CREPIN-LEBLOND: Yeah. In Durban, the GAC and the ALAC came together. The ALAC notified the GAC during the meeting and then a joint statement was sent. I guess the Board has to listen at that point.

ROD RASMUSSEN: I think we're good if there aren't any more questions on the EPDP, other than hallway conversations.

Okay. All right. Well, thanks for your time. I appreciate you letting us go a little over. Lots of questions, obviously. Again, a lot of the issues that are our concerns are ones that your folks are bringing up. Please keep bringing them up to us. We started topics or refined what we've done based on a lot of input from ALAC and of course the wonderful members you have sent us over the years. Thank you very much.

MAUREEN HILYARD: Thank you very much, Rod [inaudible]. I have to say that one of the things that I actually raised was, having read the report – it's probably one of the first reports I've actually read – I looked at it with a bit of trepidation because I thought, "Am I going to be able to understand it?" but I found it really, really interesting. There we go, Kristen. And that's why it was raised. Thank you very much. It's been an interesting session.

ROD RASMUSSEN: That was the objective. Thank you for that feedback.

MAUREN HILYARD: We're going to finish up a few minutes early. Thank you very much for the interpretation and the techy stuff and everyone else for being here. Great. Have an early break.

HEIDI ULLRICH: Hi, everyone. The next meeting here will be at 10:30, and it will be an At-Large policy debrief: What impact did At-Large make this week? So that's in 20 minutes in this room. Thank you.

[END OF TRANSCRIPTION]