BARCELONA – SSAC Public Meeting
Wednesday, October 24, 2018 – 17:00 to 18:00 CEST
ICANN63 | Barcelona, Spain

ROD RASMUSSEN: Alright. Good afternoon, everybody. We're going to start here in just a second.

Okay. Welcome, everybody. This is the open SSAC meeting for ICANN 63. I'm Rod Rasmussen, ICANN chair. Julie Hammer, ICANN vice chair. I'm not going to do introductions around the room, but if SSAC members could raise their hands. Okay. That means we're actually outnumbered, maybe. There's about 50/50. That's good. Is there anybody in the room who has never been to an SSAC meeting before? Okay, we have a few. Very good. Thank you. Welcome, first-timers.

So, I will go through the intro. I was going to hopefully skip that because you're all veterans, but that's great that we have new folks in here.

This is the agenda. There actually is … We will cover the name collision analysis project as well. We added that slide later, so that's not here, but we're going to talk about our publications after we do a brief overview of SSAC itself. Then, talk about some other things that have been going on with SSAC over the past several months. Then, have some time for anything else that folks want to bring up. Oh, the clicker wasn't working. Did I turn it off? It stopped working. Oh, there we go. As soon as I looked away, it changed. Who's behind me doing that? Uh-huh.

This is just a brief overview of who we are and what we do, etc. Currently, we're at 39 members. We have a lot of expertise from various areas, obviously focused on DNS and the various technologies and operational things that are necessary in the ICANN environment, but we go beyond that and understand other technologies as well and bring in a wide range of folks to be able to bring emerging security threats and emerging trends into the SSAC so that we can update the community and advise them when there are things to be concerned about and try and anticipate some of those things.

We do report directly to the board on matters regarding SSR, Security, Stability, and Resiliency and obviously with a focus on the addressing systems. But as I said, we do look at other emerging areas.

We have now 103 official SSAC documents, numbered series. We do have other correspondence that we have as well. But those are the main reports with recommendations. Whoever is in the back, click it for me. There we go.

This is a little bit more around the processes. The main one is the one on the lower left there, how we put together our papers and our documents. Of our 39 members, not all of them work on all of our tasks. We form work parties which will be a group, and it can be a small group of I'd say six people or so up to we've had some work parties which included all SSAC members, but typically if we have a large group it may be like 15 members.

We'll have a topic area that we're interested in. The people on that will either be experts in that area or have some interest in that area, then

they will bring various information they have. We may go do a little bit of original research of our own or ask staff to assist with that. Then that work party will meet and discuss the topics and start writing a report. Then, the work party itself will iterate on that and come up with the findings and then some recommendations, potentially. Not all of our papers have recommendations. Which will be reviews by the work party and then presented to the entire SSAC.

The SSAC as a whole will then review those and come up with its questions and may send it back to the work party for some clarifications and updates and then we will publish what the full SSAC approves. Those are consensus documents of the full SSAC.

If we do have some dissents or people who may have some sort of conflict of some sort, they may withdraw or they may disagree or have some position that's slightly different or what have you, then we will publish dissent within that document.

One of our recent documents had some dissents in it which has brought up some questions around the community. Usually, we don't, but we actually have had several in the past that have. We consider dissent to be a really good thing because that means that there's a variety of opinions and sometimes these very technical arguments or things that look at risk management, for example, have different opinions on it and we want the community have the full breadth of our thoughts on whatever the topic is.

As you can see, we put some advice to the board and the board then goes through its process around acknowledging that and then issue a

formal resolution and may direct ICANN Org to do some work or there may be some other advice to other parties that are not within the ICANN sphere, etc. Those would be things that Coms group would take care of for example. Okay, we'll try again. There we go. Am I clicking it or is that somebody in the back? Okay. I'll just put this over here. Alright.

So, here's the recent publications. And we're going to go into those. That's just a list here. Then there's some information on this slide. These slides are, I believe, these are all publicly available because this is a public session so you can get the contact information from there that of course you probably can't read from there. Click!

First, we have nobody in the room that is on this slide, unfortunately. So, we have their pictures. Many of you know Ram Mohan. He spent the last basically ten years on the ICANN board as a liaison from the SSAC to the board. He is stepping down with this ICANN. I believe he is done as of tomorrow morning, something like that. The new board is seated. Then, Merike Kaeo is t starting and she will be representing SSAC going forward. So, we will see a new person on the board from SSAC. And if you don't know Merike, which I find that hard to believe because she knows everybody it seems like, but if you see her, go introduce yourself. I'm sure she'd be happy to meet you. Click! Hey, we got this.

So, here's some of the current thing we have in process. We'll get into all of these things at the top, the name collision project, etc., further in the deck. We'll point out we gave a talk on Tech Day, ccNSO Tech Day, on IDN homographic attacks. That was our emerging security topic discussion here. That should be available at the ccNSO Tech Day

wherever they have that on the website. You can always ping us for that. That was an interesting theoretical thing that is now reality. If there's questions at the end, we can talk about that a little bit.

The DNSSEC workshop, which hopefully many of you were able to attend today. We're big participants in that. Then, of course, we have our membership committee.

I just want to point out on the membership committee we are always looking for new members. We're always looking to increase our diversity as far as technical diversity, obviously geographic diversity, and all the other diversity issues that ICANN community is looking for in general.

I want to speak to a couple of those, in particular. Technological diversity is probably our primary criteria for looking at candidates. Do you bring something to the table that we either don't have as expertise that would be applicable or that we are short of expertise on? That's something to take a look at. If you're interested in joining SSAC – and we welcome anyone to try and join – take a look at the backgrounds of the people on the website and see if you might be able to add something that we are missing.

The other thing is, on the geographic side, one of the real important things that we realize is that different kinds of security threats manifest themselves differently in different parts of the world and we're very anxious to get more members, especially from developing countries, etc., where the natures of attacks are much different than they are [and] the natures of responses and the kind of infrastructure there was

different than the North American and European traditional central area of IT. Click!

So, here are the things that we're possibly going to be taking on. This is kind of where it gets a little more interesting. The first one is we're going to be looking at our own working processes. The reason we are making this a priority is around the recent changes we've seen and the types of requests we're getting from the board and from the community. People are looking for us to weigh in on particular issues and maybe in some sort of timely fashion. We were asked to look at the KSK roll which we'll talk about here in a little bit in a fairly narrow timeframe, for example.

As I explained earlier, we have a fairly heavyweight process for looking at the work we do which includes [inaudible] a work party and all the work on editing, etc., of the publication. So, what we're trying to do here is be a bit more responsive, potentially, to the community and allow for us to be a little more flexible in how we do things and also just in general you need to look at your processes. And this ties into the independent review which is finishing up right now where there are some recommendations coming out of that as well.

So, beyond that, on the technical side, we're looking at the various Ds, [Deprive, Dot, and Doe] as a potential work party for these issues which obviously may have affects within the ICANN world and obviously the world of DNS. We also have an interest in taking a look at the hyper local root issues and what are the pros and cons of doing that. That obviously has some impacts on stability and resiliency, if not security.

Then, of course, there are areas that I think were discussed today at the DNSSEC workshop around key management and registry/registrar handoffs and the like. So, if you were at the session today, I think Steve Crocker covered that today. I was at the GDPR session today. Did Steve cover that?

RUSS MUNDY: There was a whole panel on it.

ROD MASMUSSEN: A whole panel. Okay, great. So, that's an area that we are likely to take a look at. Best practices around handling take-down procedures. This is particularly in response to large-scale take-down operations which may be a botnet or domain generation algorithm-based attack where we see a lot of variance in how people handle those things. We may have some thoughts on how to better do those and standardize some of those a bit.

There's a few things that have popped up and some of the new TLDs that are specialized around some security concerns where we may weigh in on a couple of things there.

Then, one of the things that we mentioned in our discussion with the board yesterday is we're concerned about some of the new TLDs that had very high rates of abuse within that particular TLD. To be clear here, the new TLDs in general actually had a very good track record when it came to abuse within them, dot-brands and a lot of people wanted to keep very clean name spaces.

So, in general, the new TLDs as a whole were actually safer than [inaudible] TLDs from an abuse perspective. But some of those new TLDs – excuse me for a second. I hope I can make it through this. Julie, I may call on you here in a bit.

Some of the new TLDs have extremely high rates of abuse. Over half of the domains registered in them were found to be spamming or involved in phishing, malware, and the like. So, we really want to understand that as part of our job as SSAC but also to inform any subsequent round of new TLDs. We don't want to repeat the same mistakes that led to these large-scale abuses. And this is really important from looking at things from a universal acceptance perspective, where if you have TLDs being blocked entirely, because of high rates of abuse, that's bad. And even worse is there are a lot of network operators and people looking at anti-spam solutions and things like that that are more likely to just block any entire range of new TLDs just because they don't want to take the time to know the difference between them. So, we're quite concerned that another round, if you don't solve these problems, the domains themselves or the TLDs themselves will have difficulties, regardless of how they do their anti-abuse measures. Next slide, please.

Okay, good. I get a chance to rest my voice for a second. Russ wanted to talk about the KSK rolls. I'm going to hand that over to you.

RUSS MUNDY: Certainly. Thanks, Rod. Next. As most people in this room are aware, a KSK roll did occur earlier this month or it was the main event started earlier this month. But prior to that, the board asked for advice of three

of the committees, the RZERC, the RSSAC, and the SSAC. They were really asking for input and advice on the content of the updated plan.

So, all three committees did respond, and if one wants to read those responses, they are available on the website. But generally, they were a fairly consistent response. The decision was made to proceed with the plan and the roll occurred earlier this month. Next, please.

In SSAC 102, which was our document that commented on the request for advice that the board sent us, there was … The way that the advice came from SSAC, the wording indicated that SSAC did not see any reason within our scope to not proceed with the rollover. SSAC also advised that actions be undertaken as soon as practical afterwards to address the framework for future rollovers and then a statement about the general fact that this was a risk assessment decision, the final decision, which rested with the board. Next, please.

That was the consensus opinion. There was a dissent opinion that was part of the report and it's contained in the report. Essentially, the dissent was tied to the fact that some people in SSAC made a different … Their personal judgment was somewhat different in terms of the risk of delay versus the risk of going forward than what the consensus of the SSAC, the larger SSAC as a whole was.

So, this, we think, is as Rod said earlier, a very good thing because it does give the community a chance to see some of the different perspectives and especially when there are things such as making an assessment about risk of one action versus another action. So, it gives people in the community a chance to read two different views of what

the SSAC members may think, but the consensus itself did say proceed forward. Next, please.

ROD MASMUSSEN: Thank you, Russ. My apologies. I should have paused and asked for questions after that first section on our new work, if there are any questions. I wanted to take some questions after each major section here. If anybody has any questions for Russ on SSAC 103 and any questions on what I presented earlier on topics for new work. Go ahead and come up to a mic. Or do we have … Thank you, Steve. We like questions, by the way. It's good to get feedback.

FARELL FOLLY: I'm Farrell Folly. If I understand you well, we can now have some question about the past slide, I guess. I come from the Federal University of Munich. I'm a PhD candidate in computer security related to Internet of Things. I' curious to know more about any IoT security related issue you are dealing within SSAC or ICANN community, anything related to DNS that's IoT security related. Thank you.

ROD MASMUSSEN: That's terrific because that's going to set us up for like three slides from now because we actually have that in here. So, if you'll just … If you have questions after you see that one, then terrific. Anyone else? Okay. So, let's click. There we go.

SSAC 103. SSAC 103 was actually a response, a public comment response, for the public comment period around subsequent procedures PDP. We categorized two different types of responses we made within that document.

The first was an overall meta response where we expressed our concern around the speed at which things seem to be moving with subsequent procedures and some assumptions that were being made around the inevitably and the near-term of another round.

Those comments were based on the fact that of course we have the NCAP project that we've been commissioned to do, or the board requested to do out of the board, as well as some of the items that have just been published in the CCT Review final report where they had brought up some pretty significant SSR issues that should be addressed. We also note that not all 2012 round has been resolved yet. So, that was more of a measure of concern around making sure that people understand the risks of moving forward without completing these things and addressing some of these issues.

SSAC is an advisory committee. We have no way of making decisions around this. We can just provide our advice that these things should be taken a look at.

Other comments that we made were around particular areas where they had gone through and looked at other work and we made some clarifications and provided some other links, etc., to work that had been done on this list of topics you can see underneath that.

We also noted that the subsequent procedure PDP team had done a really good job of going through and looking at past SSAC documents and others that were related to SSAR issues and were pretty darn thorough about making sure that those were included. In general, I've done what we thought was a pretty good job of analysis. So, really, the comments we made here were I think clarification [inaudible] in a minor way, for the most part.

The one at the very bottom, though, was one area that touches on what I talked about before with a potential work party. That is to name domain name abuse which the PDP did not touch on which we were concerned – actually, quite concerned about, given the results that had happened in some of the TLDs which we pointed out and believe that that should be covered in a final report. As I said, we are looking at doing a work party on that ourselves.

The DAAR project, which those of you in this room decided to not go to, to come to our project and our presentation here, is a source potentially of some of that data and information but there are other areas where we may be able to get information.

Questions on SSAC 103? Bruce?

BRUCE TONKIN: Yeah, Rod. Earlier on you mentioned that there was some new gTLDs that had a high incident of abuse. Have you done any work to look at what the characteristics of those are that generates that situation? For example, is it because they've offered registrations for free or is it

because they've used different registrars and those registrars don't have any billing, checking processes? What are the characteristics of a TLD that has high abuse?

ROD MASMUSSEN: So, that is what that work party would do is take a look at those factors. Several our members have looked at these things. My former background was in operational security as you know, but not the rest of the folks in this room. A couple of factors [inaudible] seems to be potentially one of the factors. Backend registry may be involved in some of these. Not backend, I'm sorry. Let me restate that. The [owning] registry seemed to be – there was a high correlation at least with some of the TLDs that were highly abused. I don't want to name names at this point, obviously. There needs to be some study done on that. But those are some factors.

Whether or not there are safeguards in some particular registrars that were not using good security practices or what have you may be a factor as well that has been in the past, obviously. I think that the work party will dig into that and try and make sure that those kind of anecdotal inputs are turned into something that we could actually use and get real data around it to support that. That's why tools like the DAAR an important thing to be able to reference as a collector of lots and lots of data that you can analyze. We have several members that have some relevant backgrounds and be able to take a look at that. Any other questions?

Okay. Internet of Things, as requested. Cristian?

CRISTIAN HESSELMAN: Cristian Hesselman with SSAC. The IoT Working Group is basically currently writing a report on the role of the DNS in the Internet of Things. Our goal is basically to de-hype or de-buzzword the term a little bit by explaining what the IoT means for our industry.

To accomplish this, we developed a model of how we think that IoT devices and all kinds of gateway devices in the infrastructure will be used in the DNS to find backend services. So, that's one part of the discussion and part of the report.

The second part is where we basically look at opportunities and risks for the DNS and an opportunity in our opinion is that the DNS security functions, like DNSSEC, can potentially contribute to further increasing the security of the IoT as an application of the Internet and the potential risk that we're looking into is that software developers of IoT devices may use the DNS in a DNS unfriendly way which can result in large-scale traffic increases if there are billions of IoT devices out there.

So, this is something that we're exploring in the report. It's not a formal advisory. It's an SSAC report, so it doesn't need any board tracking and that sort of thing. It's just to explain to the ICANN community and board how we see the role of the DNS in the IoT. We're currently drafting the document within the working group and we expect to publish it by the end of the year.

ROD MASMUSSEN: Questions? Okay. Click! The Name Collisions Analysis Project. Jay is not in the room, so Jim, would you like to cover that, please?

JIM GALVIN: Yeah. Interesting. So, Jay and I actually co-chair. I'm Jim Galvin. I'm not quite sure why you don't have two names on that list.

So, the Name Collision Analysis Project – NCAP, and that's what we'll refer to it here in this discussion – is been set forth by the board. I think that's probably an important point to remind people about. The board was pretty explicit. It had quite a resolution that it had passed pretty much a year ago at the last general meeting, being very explicit about the questions that it would like an answer to and it asked for SSAC to respond to those questions and propose a method by which it would respond to those questions.

So, what we have done and has already been published once in the community is we proposed a project with, in fact, three studies and we proposed a methodology in there that was intended to be thorough and inclusive that would allow us to answer those questions involving not just ourselves but also experts in the community and other technical experts. So, it was not intended to be an exclusive activity. Is there another side? Next slide.

So, the first project plan was published in March of this year. It was put out for public comment. It had been submitted to the board just prior to that and then it was put out for public comment. We actually received quite a large number of comments and we want to thank the

community for that. It was really quite remarkable and thorough and we appreciate that people put as much effort as they did into reviewing this project.

Over the summer, we have created a response to those. In fact, if you were just at the public NCAP meeting that happened just prior to this, we carefully reviewed all of those public comments and we went through all of our responses to those comments and went through them. That report should be available soon. You'll see our comments.

We have also gone, acted, on all of those comments and created a revised project proposal which is now with the board, and along with that revised project proposal, we have added a revised budget which is actually kind of nice. It came in a little bit less than the original $3.6 million that was proposed. And all of those details are currently with the board.

The other thing that I'll call out here for which there is no slide is there was one other recommendation that we had made to the board which is part of what the BTC is reviewing. We believe that with have, in sync with the board and that this is all going to be accepted, but we have proposed a new management structure for this project in response to many of the comments that we have gotten from the public comment and the initial reviews.

If you were in the NCAP meeting just an hour ago, we actually reviewed this in detail. But the short version is just that SSAC has recognized that this project is more than SSAC really is suited to complete by itself. It really is a project with very specific deliverables that are due on a time

table and it has some fairly detailed business-level requirements that need to be addressed.

SSAC is really a technical analysis body and so that would be the strength that we would contribute and bring to that project. So, we've created – proposed to the board that ICANN Org should actually be the business manager sponsor of the project and take on the responsibility of managing all of those externalities and the usual project management side of this and SSAC instead would focus on providing technical input and guidance, in particular to the statement of work that gets accomplished, and of course in review of the data and providing its recommendations to the board. But you can look for more details about all of that in the slide deck and recordings and presentations from an hour ago. That's it. Thanks.

ROD MASMUSSEN: Questions on NCAP? Okay. Moving on. Lyman? Okay, great. Take us away for talking about the review.

LYMAN CHAPIN: Thank you, Rod. SSAC is one of the groups within ICANN that is currently undergoing one of the five-year regular institutional reviews. We have completed the process of working with the independent examiner and the independent examiner has published a final report after a public comment period.

At this meeting and on other occasions, we've been discussing the recommendations from the examiner. None of the recommendations is

dramatic in the sense that it would have a huge effect on the way SSAC operates, but many of the recommendations were considered by the SSAC itself to be extremely useful, and in fact, in several cases, we intend to go about implementing the recommendations before anyone necessarily has to come along and tell us that we should.

The next step in the process will be to write an assessment report. This will be a report from SSAC responding to the independent examiner's report. Following that, we will form an implementation planning team and the idea there is to come up with the details of how you would go about actually implementing those recommendations perhaps as modified by the assessment report that everyone agrees should be implemented.

So, this implementation process can take a long time, because for the most part – and in fact, I can say without any meaningful exception – the recommendations from the independent examiner were favorably received by the SSAC. We don't expect there to be a long delay in implementing them. So, in the case of this review, and those of you who are familiar with the review process know that this isn't always the case, in the case of this review, we probably will complete the implementation phase within calendar year 19 which will be dramatically more quickly than has happened in other cases in the past. We'd like to thank the independent examiners from The Analysis Group, by the way, for the work that they did. We, as an advisory committee, found it extremely productive to work with them and we look forward to going through the process of implementing some of the recommendations that they've made. Thanks, Rod.

ROD MASMUSSEN: Alright. Questions on the review? Okay. Turned myself off here. Julie, on the other publications.

JULIE HAMMER: Thanks. So, as well as focusing on that technical work, we are of course a member of the ICANN community, and from time to time, it's appropriate for us to comment on issues that the community are considering. We have now a different series of publications that we've produced that are really more correspondence under a different numbering system. We've just picked on a couple of the more relevant correspondence items to just mention to you here.

Continuing on the theme of reviews, there have been a couple of proposals put out by ICANN Org for community comment on how do we actually deal both in the short term and the long term with this plethora of reviews that are being undertaken in the community, some of which require the participation of representatives from all of the SOs and ACs? And being one of the smaller groups within ICANN, this becomes pretty challenging for us to actually participate in that many groups.

So, we have commented on the proposals by ICANN Org on both how we deal with these issues in the short term and the long term and basically we're supporting a set of principles that might go into the bylaws as an amendment that actually gives a little bit more flexibility to the community to actually allow reviews to be potentially delayed or

rescheduled in such a way that relieves the stress on all of us in the community.

At the moment, one of the results of bringing in our new bylaws after transition is that, whereas in the past, ICANN could go to NTIA and seek some relief from the timescale that reviews were required to be delivered in. That is no longer the case because that NTIA relationship isn't there and the bylaws do not allow for flexibility. So, there are some issues there that we need to work on together to see how we'd better do that in the future. Next slide, please.

The other major body of work that's been done in the community is, of course, the cross-community working group on accountability and SSAC participated in that and we have already approved the final report of the work stream two body of recommendations. So, any questions on those issues? Thank you.

ROD MASMUSSEN: Okay. That gets us to the final slide on our deck. Hopefully, the most interesting part of this, which would be interaction with you, the folks who have been kind enough to come and listen to us and join us, actually, not in the windowless conference room. We actually have a window. Maybe that's why everybody is in here. We can actually see outside. So, any comments, inputs to us on what we're working on and items that you would like us to consider that you didn't see on our list or that you've known we've worked on in the past and may need to update? Anything like that? This is the time for the rest of the

community to give us some input beyond just grabbing us in the hall or sending us an e-mail?

JANOS SZURDI: My name is Janos Szurdi. I'm a PhD student in domain registration abuses.

ROD MASMUSSEN: That's a PhD?

JANOS SZURDI: Well, hopefully. We'll see.

ROD MASMUSSEN: Okay, cool!

JANOS SZURDI: Basically, my question is I have seen some more [issues], domain registrations that have basically been the same for years. They exist. They are blacklisted by some black lists, but not by [many] others. You can go to youtube.com, without the Y, and you will very likely see a phishing page or a scam page. It kind of changes over time, but I always bring it up as an example on cybersquatting.

I was wondering if you ever thought about it. Probably you did. But I'm just asking could you force somehow the removal of these domains that are so known to be malicious? The reason for this is maybe blacklisting

is good. It decreases the effects of these malicious activities but it kind of has been shown that if you remove a domain, the incentives for re-registering them is much slower. It's much less profitable after that. So, actually removing domains are much better than blacklisting them. This is one. Another, it has been [inaudible] for very long and I bet there are many more. This is [my impression]. [inaudible].

ROD MASMUSSEN: Most of our experts in this particular area are actually at the DAAR meeting right now. I'll go ahead and answer this. One of the items we do have on the list of future work are best practices around take-downs. The question on removal of domains is a field that has had a lot of work over the years in communities like the Anti-Phishing Working Group, M3AAWG the Messaging, Malware, and Mobile Anti-Abuse Working Group. Did I get that right, Chris? Okay. I got the right order of the Ms.

So, there have been actually several documents published around practices there when it's appropriate to use the DNS level basically for removal. So, there are actually long outstanding programs by various companies, brand holders, anti-abuse companies, your anti-virus companies, etc., which routinely go out and have domains removed.

That being said, sometimes you do see these longstanding domains that may be blacklisted. It really depends on the type of abuse that's going on on them and whether somebody is tracking that and has the authority or even cares to make a complaint.

On the flip-side, on the receiving side, is the registrar typically or maybe even a registry where they may take a look at the complaint about that particular domain name, and depending on the nature of their terms of service and other factors that weigh in like the country they're in and the legal regime they work under, they often, depending on the abuse, will remove the domain. They just need to know that it's there. And when you say phishing, that's pretty universal. Those will get taken down.

When you get into trademark areas, they're usually looking for a trademark older to do some sort of official action that will be more in the legal arena.

So, it really then depends on what kind of abuse is going on, but the responses do vary as far as the ability for companies to do something or registrars or registries to do something about that. And for— [audio cuts off].

[END OF TRANSCRIPTION]