DUBLIN – SSAC Public Meeting
Thursday, October 22, 2015 – 08:00 to 09:00 IST
ICANN54 | Dublin, Ireland

UNIDENTIFIED MALE: This is the SSAC Public Meeting in Auditorium Room on October 22, 2015, from 8:00 AM to 9:00 AM.

PATRIK FALTSTROM: Okay. It's 8:00 so it's time to start. Welcome, everyone, to this open meeting for SSAC, and we are going to give an update on our activities. I'm happy that you arrived so early, so I understand you queued up to be sure that you got seats. So support staff, you can now start to let the people that have sort of waiting tickets into the room because we have some seats left.

We do have some SSAC members that, unfortunately, due to conflict across other meetings, including CCWG, start at the same time, and also the ICANN Board. So some people, unfortunately, are not here. We'll give an overview over what we are doing, our progress, what we have done lately, and we will specifically talk a little bit about SAC 073, the root key rollover, registrant protection issues, and last, give our normal update and request for feedback.

EN

We have a new way of presenting ourselves that we are trying to test at this meeting for the first time to explain a little bit to the community where we are, which is kind of important to know when we are participating in the CCWG, when the different SOs and ACs are asked how they are participating in the work or the community.

We have a charter and the charter says that we are SSAC is here to advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. That's how a charter, which is in the bylaws of ICANN.

We have 73 publications since 2002, and they are both reports, advisories, and comments on, for example, the open comment periods that ICANN is running. We have 35 members and we are appointed by ICANN Board.

We have a wide variety of expertise, and our Membership Committee that I will describe a little bit later is trying to ensure that we have the expertise that we need for the next couple of years, and at the moment, you see on the list here, the various expertise areas that we do believe we have and that we need.

The charter of ours that we are to look at the security and integrity issues related to the addressing systems and identifiers is matching the mission and core values of ICANN, which you'll

ICANN | 54
Dublin
18-22 OCTOBER 2015

see up to the top left. The mission and core values of ICANN include to ensure the stable and secure operation of the Internet's unique identifier systems and also to preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet.

So we interpret our charter as being an advisory committee that specifically is looking at the mission and core values at ICANN. And based on those two matching each other and sort of a stress test of the various statements we potentially make in the form of advice, we might publish documents and advisories, which includes recommendations.

In the case that what we are saying, our recommendations and to the ICANN Board, you see the [inaudible] to the right where we are submitting the advice to ICANN Board. This is after the advice or at the time when the advice is published.

The Board acknowledges and studies the advice. It takes formal action on the advice, which can be one of four different paths in general terms. Either launch a PDP or ask staff to implement whatever we are recommending with the help of the normal public comment public consultation processes according to similar kind of changes that are initiated by ICANN Board.

It could also be a dissemination of advice to affected parties. For example, it could very well be interaction with other

organizations like W3C, IETF, ITU, CA/Browser Forum, and similar. Or it could also be that the Board chooses a different path – a different solution – where we expect to get an explanation why the advice was not followed.

The recent publications, of course, include a number of publications due to us being a chartering organization for the various activities that is ongoing related to the IANA transition issue, and that includes the SAC 071 and 072, but it's also the case that we just recently issued a report on number 073, which are comments on the root zone key signing key rollover plan.

We have a webpage, ssac.icann.org. We also try to let everyone that uses Facebook know what we're doing, and we have started to make videos to explain our reports. So for those who would like to have a look at that. We also have a new logo.

So let's talk a little bit about what we are doing and what we are going to do, what we plan to do in the future. So these are the work items that currently ongoing. We are looking at a potential next round of new gTLDs and what we're doing here is that we are reviewing the advice that we have given so far, what effect they have had if they have been taken into account, if they have been implemented. If it is the case that something that we have already talked about but has not really been implemented fully must be implemented before the next round, whether we have

ICANN | 54
Dublin
18-22 OCTOBER 2015

different things to say this time, whether we think that some advice we gave are no longer critical for the process, etc.

So the first step for the work party is really concentrating on looking at what we the issues we have been working at and what we have been talking about in the current round to evaluate those for the next round.

And by the way, one of the reasons why we start this early is that we think and we know that some of our advice… Either we released advice too late in the previous round or released them in a way, even too early, in the current round so that the effect was not as high as it could have been or created issues in the process itself. So we really want to be ahead of the curve here this time.

We have one work party that we'll talk a little bit about later: the registrant protection credential management. We'll come back to that. We will have a workshop at the Internet Governance Forum in Brazil, which will be based on the work we are doing in credential management. It's a panel we are going to have there.

We have a workshop. We have had a workshop at the IGF for the last couple of IGF meetings with different topics. We just launched a work party on IPv4 address exhaustion, which is because we are not only looking at DNS, we have been looking at the routing and IP address allocation for quite some time, but

now we see that when we're running out of IPv4 addresses, it's really the case that there are some serious issues going on there and we are investigating whether something can be said or should be said that can help the current situation.

When we have a work party, let me just emphasize that because we got some questions specifically from people, individuals, also active in the RIRs – just because we have a work party doesn't mean that we will issue any kind of advice. We're just investigating whether we are going to say something.

For me, as the chair, one important thing is that we are not just – SSAC is not a group that just talk about what is a problem. We speak up when we think that something can be done by someone to make things better. So that we have issues with IPv4 exhaustion. Everyone knows that. We don't have to say that. But maybe it is the case that something that we believe that something should be done by someone. In that case, we speak up.

We have the DNSSEC sessions at ICANN meetings. We have a DNSSEC for newcomers on Monday. We have a large DNSSEC workshop on Wednesday, and that happened also this time. We are overviewing and working together with ICANN to come up with ideas on better document management tools when groups like SSAC is producing documents, and that includes, of course,

ICANN | 54
Dublin
18-22 OCTOBER 2015

the ability to work with staff editing and receiving comments and the whole internal process. So we are spending some time with that at the moment together with ICANN.

We have launched explicit work on Board advice tracking, which is the picture that I just displayed. No. Come up here. You're an SSAC member. Yeah, these chairs are a little bit more comfy, but you are to sit here. Good morning, Andre.

So one thing that is really important that we have seen is that some of the advice we are given has simply been dropped because we have forgot about it, staff has been forgetting about it. So without pointing fingers at anyone, things that have been complicated to do something about, I will talk about one of those examples shortly.

It is just a lot of work to keep track of things, and specifically after half a year or a year, okay, so what happened with this advice? Trying to go back and e-mail and tickets and information all over the place, and try to understand what actually happened with a device is very tiresome.

So David Conrad and ICANN have us a task to come up with both a better process, a well-defined process for advice to ICANN Board and that is from all advisory committees, but he's working specifically with us and ALAC because we have a little bit more clear recommendation than some of the other ACs.

And then given the process also an online tool that can be used for following that process. And we're working together. We have the staff on that. And then we have an ongoing membership committee, which is like a nomination committee that looks at the skillsets that we believe that we need, and also evaluate individuals that have applied to become members of SSAC.

If we look at the milestones, we just published SAC 073 in the third quarter, and we are looking for releasing the advice on registrant protection credential management, and just because it's tied to the IGF, the timeline here is really to publish this in time for IGF, which means that we hope that it will be released in the next few weeks. Q1 2016, we envision to be ready with advice on new gTLD program review, and also how DNSSEC workshops at ICANN 55.

So SSAC comments on ICANN root zone KSK rollover plan, SAC 073, which was just published. I hand it over to you, Russ.

RUSS MUNDY: Thank you, Patrik. So there is a design team established a few months ago to do an analysis, produce a report, on the root key, key signing key rollover approach. And in our monitoring of what was going on, there were some questions that were raised by the SSAC members about what relationship there was and what pieces of recommendations from our earlier SAC 063

publication, which was published in February of 2013, and then went through the Board process and was… The old version of the Board tracker said there should be response by March of 2014.

But this particular design team for the root KSK rollover did not have a relationship that we could see in any obvious ways. So we asked the question. The SAC 063 recommendations dealt with… Generally discussed the key management for the root zone, the motivation for root KSK rollover, risk associated with it, and trying to begin the qualifying of what the risk means if you do have a failed rollover.

And so in 063 –SAC 063 – there were five specific recommendations. It's not a complete – it's not intended to be, nor was it ever thought to be, a total analysis of what all the problem set in the detail description, but we were actually hoping that the design team would have had more correlation between what SSAC had to say and SAC 063, and the publication that was put out.

And to a great extent, that is the focus of SAC 073 to ask that the design team make some type of correlation between the recommendations in SAC 063 and SAC 073, and their comments about the SAC 063 comments would be of value to SSAC because if some of the recommendations that were in our report

were no longer valid or didn't make sense, there would be absolutely nothing wrong with that, but we would like to hear on either a positive or negative sense what did the current design team work think about those recommendations.

PATRIK FALTSTROM: So the next thing that we are talking about is the registrant protection, the report that we hope that will be finished shortly. I hand over to Ben.

BEN BUTLER: Thank you, Patrik. So this work party has struggled a little bit with identifying the correct scope for this paper because, as you are probably aware, credential management is an extremely large problem and it affects pretty much every aspect of not just the DNS and namespace community, but all online service providers.

But we wanted to focus our recommendations on identifying the problems that are happening all through domain name registrars, registries, and with the registrants to see if we can identify best practices that would actually help move the ball forward, help get the registrars, for example, who are struggling with getting better credential management processes going, see

what their hurdles were, and what we might be able to do as an ICANN community to help resolve some of those problems.

So as Patrik said, we're trying very hard to get this published. We had hoped to do so before this meeting, but that wasn't really an option because our default position is always that we want to publish the most correct and the most valuable paper that we can – not just on a particular time schedule. But we are very close.

We're looking at recommendations that would provide some advice on the usage of statistics and breach reports that are currently available to the community in such a way that we might be able to detect threat actor patterns, trends, and tactics that are going on so that people in the registrar and registry community can better protect themselves.

We're also looking at recommendations concerning registries and most importantly in the document, we tried to identify a very thorough section of best practices in the general credential management from the designing and implementation phase all the way through the destroying of credentials and how those should be properly managed. So we wanted to make sure that we had a thorough best practices that people can use at an operational level and we want to work with ICANN on education

ICANN | 54
Dublin
18-22 OCTOBER 2015

to help get those best practices disseminated to the widest possible audience.

We will address in the document, as I said, the best practices for the entire life cycle, and we also tried to identify all the credentials that are used in various situations in the namespace environment and in the domain name ecosystem specifically. And we also wanted to identify specific problems that, through conversations and working with the various parties involved in this, what are the major hurdles? So that people who are getting up and running can try to avoid those before they run into them.

PATRIK FALTSTROM: And then on the last thing we would like to mention is that we're always happy to receive input on how we should prioritize ideas on things that we should look at, explicit questions that we should answer from anywhere in the ICANN community, not only ICANN Board. So the other SOs and ACs are welcome to send the questions to us.

We also are happy to get feedback on how to disseminate our information, for example, that we are trying to communicate using videos that explain our reports is something – is a request we got from ALAC, and they are very happy with the way we have tried to use to video to explain what we are doing.

ICANN | 54
Dublin
18-22 OCTOBER 2015

We also would like to get feedback on the publications themselves. Are they too long? Too short? We're trying to write the text in such a way so that the text is understandable for the party that we give recommendations to. Yeah?

Which means that if it is the case that the audience is supposed to be or we target a nontechnical audience, then the text also should be nontechnical. If it is the case that we give recommendations to more highly recommendation to more highly technical audience, then yes, the executive summary and such should be so that people, well, more or less everyone understand it, but it's really important that whoever the recommendations target get enough information to be able to do whatever we want them to do.

We also always, of course, would like to get information about how we can do things differently. And, of course, what topics you think are missing from the list of activities that we currently have. And with that, I would like to open the microphone for all of you in the audience. I'm happy to see so many people here.

UNIDENTIFIED MALE: Hi, Patrik. So I've got about 1,000 things and big queue. Starting in reverse order, then. Community interaction. It would be nice if there were some form of mailing list that went out to anyone

that could subscribe to, to find out what's going on within the SSAC because Facebook – I don't do those types of things.

Some of us are a bit more technical focused and don't look at videos and like reading e-mail lists. And did I mention e-mail lists? I love them. So just something that will let us know a little bit more about what's happening would be great.

PATRIK FALTSTROM: Okay. Let us get into follow-up questions. We have been pretty careful to ensure that we include in our activities in the normal announcements of what's going on that ICANN is using, but you would like to… I see also on your face, expression that if we had a mailing list that you could subscribe to, that would be appreciated. Okay. Thank you.

UNIDENTIFIED MALE: Absolutely. And I'm not talking high volume at all anyway here or no interaction. It's simply a subscriber list.

PATRIK FALTSTROM: Understood. Thank you very much. That's a good suggestion.

UNIDENTIFIED MALE: Okay, then. Next thing. As you know, I mentioned I run a registry, and we regularly have penetration testing and all those sorts of

things of us, and I have a very strong, independent regulator sitting just there to make sure that I do those things properly. Okay?

ICANN doesn't appear to have the same, and in the last 18 months, we've had, what? Two breaches of ICANN. I'm surprised that SSAC hasn't established a role in oversight of some of that, some form of involvement.

PATRIK FALTSTROM: Okay. This is something which is kind of interesting, and that we'd be happy to talk with you about. Partly because of these incidents, we have quite good communication or very good communication with ICANN staff related to security, ICANN's own IT department, etc. We have made a decision that we do not oversee the internal IT and security of ICANN, just the same way we are not overlooking your security of your organization or everyone else.

What we are looking at is explicitly what we had in our charter, which is – let me just go back – there, up to the right. But based on this, what we have there to the right, of course, ICANN compared to other organizations are doing quite a lot of this, which means that if it is the case that there is some kind of event that is happening which might impact the integrity of the

Internet's naming address allocation systems, then we step in. So that is how we are trying to sort of draw the line.

Now, regarding the events that has happened, we have met with ICANN and ICANN security, and we have been briefed on those events, and some of them under the NDA that also all SSAC members have signed. So we do have pretty good insight in actually what has happened.

That said, you're absolutely right that we're not doing any other kind of testing of the software that ICANN that is used for these identifiers, which seems to be what [inaudible] understand, sorry.

UNIDENTIFIED MALE: If you go forward one slide, so top left, ensure the stable and secure operation, there is no doubt that much of what ICANN does in its operations is now a fundamental part of that. If I have a failure… So recently, we had a major power outage, took us out beyond our service level agreement time, then there is an independent report written about that.

So my suggestion is not that you are doing penetration testing or things like that, or whatever, of ICANN, but that you are making an independent assessment of how ICANN is managing its own security and you are publishing that.

PATRIK FALTSTROM: Okay. Understood. That's something we can talk a little bit outside about this, but we are having those discussions on what we actually should do. It could be everything from us writing a report when the incidents have touched the part of the operation, which have to do with the identifiers or similar kind of things like the root zone management system, or whatever.

Another thing we could do, of course, is to do sort of a matter report and describe how we view ICANN is taking care of the same kind of issues. That's something we also can do to describe to the community that we do believe that the ICANN security team and the ICANN IT department do have these kind of things under controls that we can sort of look at ICANN operation.

UNIDENTIFIED MALE: It is the matter report. I think it would be your role. The rest would be their own security team's role.

PATRIK FALTSTROM: Anyone else that would like to add something? That's also good input. Thank you. And let me once again say that we have extreme good cooperation with Ash and David Conrad and Piscitello and John Crain and those people. And we have been

moving forward. For example, in the meeting that we had I think about two weeks – sorry, a month ago or two go – we actually were sitting down in two hours just to talk about the issues, what are you doing? What are we doing? So having us come in with even more proposals of us bringing in, for example, your input, I think, is a no-brainer. We can absolutely move forward there do more.

UNIDENTIFIED MALE: Yeah, just to be clear. They're good people, they know their job, but I think structurally, it's important to have an organization that writes that matter report saying that they're doing a good job.

PATRIK FALTSTROM: Absolutely. Compared to earlier, more like a couple of years when the interaction between the community and ICANN staff was, you could say, more stressful. You see what I mean? There's much, much more cooperation now. And also, we have also got some indication from ICANN staff that having us issue those reports also helps them.

UNIDENTIFIED MALE: Okay. Good. Long queue, so I'll move on. On the registrant protection credential management, just a question as to how

much ccTLD involvement there was there or if this is very gTLD-focused when the use of the word registrar is made. Is that an accredited ICANN registrar?

UNIDENTIFIED MALE: We interfaced with both the gTLD and the ccTLD models in getting feedback on what the current state problems are and trying to identify the best practices that they might be able to employ. So when we talk about registries and registrars, we were sensitive to the fact that some are vertically integrated, and with ccTLDs, it's a very different landscape.

UNIDENTIFIED MALE: Okay. On the ccTLD technical lists I've seen, I haven't seen that outreach. Maybe I've missed it. I don't think that would undermine your report in any way, but I think that for some of the sensitivities, it would be nice if we just had just slightly more comprehensive coverage of those things that went to those areas.

UNIDENTIFIED MALE: And some of the issues are more central to, say, protocols rather than the whether the registry is a C or a G, for example. So we talked about some of the issues around using [inaudible] codes. Some of that's specific to gTLDs because of the obligations that

ICANN | 54
Dublin
18-22 OCTOBER 2015

the registrars and the registries have, but probably also have a couple [ccs].

UNIDENTIFIED MALE: Okay. Just a reminder there is effectively one model of gTLD registry and there are 50 to 100 models of ccTLD registries. So I'm not claiming that we have best practice here in any way, but I'm often surprised going out in the cc community how well someone has done something else. It's just [inaudible]. So moving on to the final thing, then.

I've spent the last, I think, about 35 years of my life writing the IANA SLE, and all compressed into one year, and I think that this is something that SSAC should consider whether or not it has a review of to understand – sorry, SLE is service level expectations. That is ICANN speak for service level agreement. It is the new proposed document for the new post-transition IANA as to how it will measure itself, record its performance, and to what SLA we'll have in place.

This is something where I think perhaps you should consider, whether, again, there is a matter report done, to look at whether there are any issues in there. There may be nothing. It may be fine, but this is a substantive piece of work and a substantive change to the way that IANA will operate. And I think that, as a

result, there is always a risk involved in that, and that risk assessment is something that you can perhaps consider.

PATRIK FALTSTROM: We will, of course, study what all the operation communities have produced, but I think from SSAC perspective, it's really important that, for example, the SLEs and otherwise service level agreements is something that operational communities come up with, and they are the ones that define what kind of services they want from ICANN.

UNIDENTIFIED MALE: Absolutely.

PATRIK FALSTROM: On the other hand, of course, that is something that we will interpret and read and learn from the operation communities what expectations they are, they have, on the IANA operations, for example, because that gives indications to us how we should tune our measurements and our sort of whatever toolbox of risk calculations so that, for example, we do risk calculation in a similar way that we could believe that the operational communities do.

ICANN | 54
Dublin

UNIDENTIFIED MALE:	Right. Some potential questions to ask are is the depth of data collection onerous and potentially going to risk anything with IANA? I don't think it is. I've specified it, so I wouldn't think that. Is the level of data that is going to be published going to expose any details within IANA that should not be exposed? There are potential questions there. I don't know if they're important enough or if they're [inaudible] I'm not suggesting that you would, in any way, write elements of the SLA. Again, it's the meta level assessment of the new SLA and how that affects the overall stability of the operations.
PATRIK FALTSTROM:	When you talk about data collection, I see immediately three different kinds of data that might be collected. One has to do with sort of the WHOIS database and whatever goes into the root zone. The second might be logs from those transactions that it might be the case that the registries actually have made. The third one has to do with specifically in the RAA, the requirements on reports or breaches and other kind of stuff that explicit reporting of incidents. Are you talking about all three of them in general terms or?
UNIDENTIFIED MALE:	Number two.

PATRIK FALTSTROM: Number two. Okay.

UNIDENTIFIED MALE: Yeah. Specifically.

PATRIK FALTSTROM: Thank you. One thing that is related to that, which is an advice from SSAC that ICANN did not follow – they chose a different path forward –has to do with how to handle namespace collision issues where we, in SSAC, recommended that a honeypot was created for high-risk names so that it was possible to actually see what kind of traffic was going to be used for these names that were to be allocated, delegated.

ICANN did choose a path forward where delegation, which have been made to 127.0.53.

53 instead where one of the reasons be that ICANN did not want that data to be collected at anywhere in the ICANN organization.

And one of the reasons that were discussed had to do with what happens with that data, the risk of breach, etc. Where we did one risk calculation, ICANN did another risk calculation, plus that ICANN had other reasons, as well, to choose a different path.

We are still waiting for the final JAS to report, which will explain how ICANN made that determination, and that will be very interesting for us to read and because, once again, it was not all the parameter. One of the parameters was clearly the risk for data being collected, what could happen with that. So keep your eyes open for that one.

So we have another 26 minutes. Any other SSAC member that would like to bring up something that we have been dealing with? Going. Going. Okay.

Thank you very much for coming at this early hour.

[END OF TRANSCRIPTION]