
MARRAKECH – Joint Meeting of the ICANN Board & the SSAC

Tuesday, March 08, 2016 – 14:00 to 15:00 WET

ICANN55 | Marrakech, Morocco

RAM MOHAN:

Welcome to this session. This is a meeting of -- a joint meeting of the ICANN board and the Security and Stability Advisory Committee. Many of the members of the Security and Stability Advisory Committee are here in front of you, in front of the board, and several of the board members are here, and doubtless others will join us. I'm going to hand off --

So this is Ram Mohan. I'm the SSAC's liaison to the board, and welcome, Patrik, and let me pass the microphone to you so you can, you know, kick this thing off.

PATRIK FALTSTROM:

Thank you very much, Ram. I'm Patrik Faltstrom. I'm chair of the Security and Stability Advisory Committee here in ICANN.

Let me start by thanking the ICANN board for having this meeting. There were a couple of years when we didn't have any real structured interaction between the board and SSAC, and I think now when we, the last couple of meetings, have had that, I think the quality of the discussions and also the value of the discussions and interactions between us have increased immensely.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

So let me just say that I think that is really good.

Let me introduce one more person here, Jim Galvin to my left, vice chair of SSAC, and then we have -- on this table, we have a number of SSAC members on both sides.

We are a total of 30 at the moment, 30 members of SSAC, and just to inform the rest of the people in the room, we are giving -- we're an advisory committee and our charter is bound to the bylaws of ICANN that talk about security and stability of the identifiers that we are using in the Internet.

RAM MOHAN:

Thank you, Patrik. I think there are several questions and topics on the agenda from the SSAC to the board, and there are also a couple of items that the board has to the SSAC.

What do you say we start with the board questions to the SSAC and then we go --

So there are two questions that the board had raised to the SSAC.

Number one, diversity is considered to be a challenge in ICANN. How is your advisory committee doing with regard to enhancing diversity in all its dimensions? What can ICANN do to support that effort?

PATRIK FALTSTROM: Thank you very much.

We in SSAC, we do take diversity seriously. On the other hand, we primarily look at the skills diversity, when we evaluate for new memberships of SSAC.

Diversity is important and a good goal and important goal in any kind of global volunteer organization, and SSAC is not an exception.

We are -- like I expressed yesterday on the open plenary, we do - - we are very careful, regarding, for example, geographical diversity, that every SSAC decision is taken by using electronic mail, so a face-to-face meeting is not important -- is not of importance for SSAC to reach any -- to -- to make -- to -- you don't have to participate on the face-to-face meetings to be able to participate in the decision-making process and we think that is important.

Regarding what ICANN can help us with, we do in SSAC try to tie onto the outreach programs that ICANN is already organizing. For example -- for example, the fellowship program, which we try to follow closely.

We have had a few -- a few SSAC members that came directly from the fellowship program, and we are looking -- we are

looking among the fellowship member -- fellowships all the time to be able to find new SSAC members.

We also think it is -- we also do the DNSSEC workshops, both introductory workshops and also the workshop for more technically skilled people, and we thank ICANN for continuing to give us support to be able to have those outreach programs.

We could get some help by -- also get some help identifying potential new leadership and participants in the -- in SSAC and in other ways, sort of continuing the partnership we have with outreach.

That said, SSAC is only 30 people so we cannot do any of these things alone. We are tying onto what ICANN is already doing. Thank you.

RAM MOHAN: Any -- any comments from board members? Asha?

ASHA HEMRAJANI: This is Asha Hemrajani, for the record.

Patrik, thank you very much for mentioning the DNS workshop. I really wanted to commend that. I think it's a great workshop that you guys run. I learned a lot from it myself, and I saw that this time when you ran it in Marrakech, you had a very large

contingent from the African community, and the feedback I got from some of them was very positive. So very, very highly appreciate it. Thank you.

RAM MOHAN:

Other comments from the board?

Okay. Let's go to the second question that's on the screen, Patrik.

What is your feedback on the final report of the CCWG on accountability?

PATRIK FALTSTROM:

We accepted without any comments the final report of Work Stream 1 of the CCWG on accountability, so there is not much to say about that.

That said, we have in our earlier documents given quite a lot comments which more is attached to the actual implementation phase.

So, that we didn't leave any comments here doesn't mean that we go to sleep and wait until the whole ICANN is restructured. We will watch this really carefully. Thank you.

RAM MOHAN: Thank you. If we could go to the previous slide, there -- I wanted to -- there are a bunch of questions. These are all come in the area of what I would consider technical areas and technical responses and questions.

Are there any other topic on the technical side that should be there? I see Jonne.

JONNE SOININEN: Yeah. Hello. Jonne Soininen, the IETF liaison to the ICANN board and also a part of the board working group on IDNs.

I -- we have -- the board working group on IDNs has an additional question that wasn't on the original list, which was related to the IDNs and second-level strings in -- working group in ccNSO where the request was, when that was created, that working group, that parties like GAC and the SSAC would be involved, and what we would like to know is: What is the involvement of -- what is the planned or current involvement of SSAC to that work?

PATRIK FALTSTROM: First, a meta-level response, and that is that SSAC makes decisions by reaching consensus, and as I said earlier, we reach consensus by having a statement that we agree on during a 48-hour, one-week -- more often, one-week -- last call via email.

That is how we make our -- or raise our positions. And that means that it's very difficult for SSAC or, in reality, SSAC cannot participate in any work like that.

What SSAC can do is to respond to certain questions. We can review the -- the document itself. We can, in general, come with comments or statements or recommendations to a work party that is working on things like that. And finally, we can appoint individuals that we think are skilled to participate.

On the other hand, that doesn't mean that they speak on behalf of SSAC in any way, shape, or form, regardless of whether those individuals are members of SSAC or not.

So that's the first part.

Secondly, regarding the ccTLDs and IDNs, we in SSAC have just launched a work party to look at the generic IDN issue and, specifically, from our perspective whether there is an issue with - with -- and if there is lack of harmonization between the various processes that look at internationalized domain names and the like, like Trademark Clearinghouse, the label generation panels, the ccTLD fast track.

So for example, the question is, for example, it's the case that the output from the label generation panel should also be instructions directly to the ccTLD fast track and vice versa, so is

there a risk and -- that you can, for example, get a new gTLD with certain characters that you cannot get in the ccTLD fast track or vice versa, and if there is a difference, does that have any impact on security and stability. We don't know.

So we are looking at that. We're going to look at that. And also the various versions of Unicode which also is something that impacts the label generation panels.

Regarding the actual questions regarding the ccTLD and that process, I think it's important not only to look at the technical issues but also the -- the -- sort of the -- the actual process itself for ccTLDs, because one could, of course, ask one's self whether ICANN actually can say no to a ccTLD or a country that actually asks for a certain string.

JONNE SOININEN:

Regardless, perhaps, of that question, the question is that being part -- are you -- because most probably the working group will need help on the security areas as well. Are you planning to use one of your methods -- which include, for instance, appointing somebody to follow that work -- to look at that?

And the other thing is also that what we are concerned -- or not concerned, but we are interested of, that you know about the

work and you have some follow-up -- following of that work, if it's needed to, for you to react.

PATRIK FALTSTROM: I got the question from Ram, the liaison, at 7:34 yesterday evening.

We have an SSAC meeting after this board meeting, and we will discuss how we're going to appoint a person or to -- to this group or not. I cannot answer that question.

But we will discuss it.

Regarding -- regarding what we are doing in the work party and whether the outcome is something that helps others, I am saying every time we meet a group, that we'd really, really like input in SSAC and we don't get enough input.

Here we did get input and we do have a work party that works on this topic, so I'm pretty sure we'll try to come up with something that actually helps.

JONNE SOININEN: That is a very good answer and thank you very much.

RAM MOHAN: Thank you.

Patrik, let's -- let's move to the other part of the agenda, which are questions from the SSAC, topics that have been raised.

On the -- on Question Number 1, Asha is the shepherd from the board's side.

PATRIK FALTSTROM: Thank you very much.

SSAC, in 2013, wrote Document Number 63, and the reason why we wrote the document is because in 2010 ICANN signed the root zone, and after some time, it -- and in the -- what is called the practice statement, there is -- there is information that there will be a key rollover and that key rollover will be happen -- will happen when needed, or after five years.

So in 2013, because SSAC didn't really see much happening, we wrote SAC63, which encouraged ICANN to start looking at the issue with key rollover, because it is a process that takes some time, and just like the IANA transition, it's something that takes some time to both make the plan and implement the plan.

We, in that -- in that recommendation, just pointed out that we think that this is actually something that we -- from our perspective, we think it should get higher priority.

We -- regarding the recommendation in SAC63, the actual issues we have here with the reason why we're not discussing the topic until now, to some degree, has to do with the fact that we, as an advisory committee, and ICANN staff and everyone involved has not really been doing our homework really well regarding tracking this kind of advice, so that is sort of --

So one of the issues here is delay and we don't really know where the advice is. But that's a separate matter that we're not talking about here.

So then in 2015, when we -- when we saw that some things were happening but not -- not that much and we started to get close to this five-year thing, we sent a letter, in the form of SAC73, where we once again pointed out that there is something that needs to be done here and we wanted to have a little bit more attention, we wanted things to move forward.

We also mentioned this to ICANN board in our meeting in -- in the last meeting in Dublin.

So from our perspective, we still believe and have always believed that it's really important that this rollover process start.

We are aware, of course, that the zone signing key, which is one of the two keys that are in use, is something that might be

changed, increased in size or whatever, by the root zone manager, which currently is VeriSign.

We also know that there's a design team that have been working on the report; that some SSAC members have been part of the -- of the team that has written the report. SSAC has been briefed on the content of the report. A report that, by the way, was released this morning. So a lot of -- so now it is possible for everyone to read what's in it.

We think -- this report includes a time line, and we think it's quite important that now urgently, there is some investigation done to see whether that time line can be met, cannot be met, and if the time line is not be met -- is not met, what in that case is to be done.

Regarding the actual SSAC recommendation and views, we just think that -- to summarize, that the signing is actually happening and -- sorry, that the key rollover is happening as soon as possible, whatever that means.

And also, that for the process of key rollover to happen, it is important that there is some kind of escalation process if it is the case that -- that some kind of breakage is happening, so that it is decided, when there are some indications, whether the indications are correct or not and whether there should be a rollback or not.

Normal pure operation, you cannot really invent that on the fly. You need to have those things in place already before. But all of that, to some degree, more or less, is in the actual design team's plan that was released today.

So this is something that we have been discussing, and also Asha and myself have been talking about that -- this for quite some time, and we in SSAC, we are happy -- let me say that -- with all the discussions that we had the last couple of days with ICANN staff and ICANN board and everyone involved and I would like to take this opportunity to thank everyone for the very good and constructive discussions. Thank you.

RAM MOHAN: Asha?

ASHA HEMRAJANI: Okay. Thank you, Ram, and first of all, thank you, Patrik, for sharing your concerns on the rollover, which you also had brought up in Dublin.

So first of all, we acknowledge the hard work that has been put into the KSK rollover preparation and the SSAC's work into SSAC -- into SAC63 and 73. And for the benefit of those board members who may not know what SAC63 is, just a reminder, it's the SSAC advisory on DNSSEC key rollover in the root zone.

So we note that SAC63, as you mentioned, was issued in 2013 and the first detailed responses from ICANN started in 2014, and this really points to a need for better communication and a tighter feedback loop.

I know staff have taken steps to improve and simplify communication channels.

Now, with the new board advice registry process just getting started, the board is focused on responding in a timely and in a complete fashion to recommendations from SSAC. And I want -- I can't emphasize that enough. And indeed, from recommendations from any SO or AC.

The board advice registry, or BAR as we called it yesterday when we were having that discussion, Patrik, will allow greater tracking of advice and should ensure this tighter feedback loop.

So in Dublin, if you recall, Steve had nominated Melissa to be in charge of -- or to be working on BAR as well as -- oh, there's a little bird here. Hello.

[Laughter]

ASHA HEMRAJANI: -- as well as David to be working on the BAR. So I understand there has been some communication on the BAR and I hope that

will close the feedback loop on that and get that running for you as soon as possible.

So as -- but speaking on behalf of the board, we -- we will continue to exercise our oversight function in this and other important security and stability matters that the SSAC brings in front of us. So thank you.

Before -- I wanted to ask if there's any other board members who would like to add to that.

Yes, Bruce.

BRUCE TONKIN:

Thank you, Asha. Bruce Tonkin from the board. Just probably worth noting because I know sometimes people think that the board members are not in the room. It's pretty much the first two rows here. So we have got a huge board, and we've got most of the board here.

On this topic, it's really the first time I'm hearing about this, just the timing of this. And I think it's always going to be a challenge. Like, whenever you try and roll over the key, there will always be the case where it's going to break some stuff. That's actually part of the point. I think it's actually probably better to do this earlier than later. If we wait another two or three years, you are going to get more and more of an install base and probably -- if

something does go wrong, it's going to have a bigger and bigger impact.

I would encourage sort of proceeding with the planning for doing a root zone key rollover. Maybe the actual time when you push the button, you might push out a little bit past some of the challenges that we've got in this particular year with so many things going on.

But all the preparation, I think we should proceed with that. Especially thinking about your communication strategy because I think that's one of the really key things to get right, that we're able to explain to the people what this means and then if something does break, people sort of have an idea of what's the cause of the breakage and that they can correct. So, yeah, I encourage proceeding.

PATRIK FALTSTROM:

Thank you. Before I invite other SSAC members to say something, that is approximately what we are saying in SSAC as well. On the other hand, there is one addition I would like to emphasize and that is that, first of all, the design team's report do include a time line that, of course, a lot of people are aware of in the operational community, which means that -- and also the other part is also sort of make their own plans in parallel with the design team's report.

So the only thing I want to emphasize from the SSAC perspective is that ICANN cannot only do the decision of their own time line in isolation. Coordination is key there to also be able to detect potential issues here.

So even if ICANN decides to wait for some reason, there might still be some actions for ICANN to do just because other parties have their time line anchored to what is already published. So "just wait" is not really an option.

Is there anyone -- sorry. "Just wait and not do anything" is not really an option. It's important from today when the report is released to keep track of where the world is.

Oh, Ram had also said what are some of the dates. So in the report, I would like to hand over to Geoff which actually was part of the design team that which could talk a little bit on that.

GEOFF HUSTON:

Thanks, Patrik. Geoff Huston also from SSAC. I had the honor to be a member of the KSK design team, so I am familiar with the report and certainly with the dates.

We are mindful of the fact that the keys are treated with due respect and care and actually only opened and used at certain times of year called key ceremonies. We felt it was appropriate to fit the key role within the existing schedule of these key

ceremonies. So the process is intended to start on the 1st of April of this year. And for the remaining seven months until the end of December, we would use that time to actually generate the new keys to be used in the key signing ceremonies, distributed to the second center; in other words, do the necessary preparation work on the key without changing any of the operational parts of the zone itself.

The start of the zone change would happen on the regularly scheduled zone management operation. The first one would be on the 1st of January, 2017. This would be announcing the new key which we believe is a non-disruptive event.

The next event would occur three months later with a switch from the old key to the new key. We believe that would be about the most disruptive event in terms of potential damage.

If there are old resolvers that do not track that movement, they will find that the DNS will go black. We are acutely aware that we do not know how big that population is. We'd like to think it's small, but we have no true feeling of how small.

The next event is another three months after when we then take the step assuming the first two events have gone without impact and haven't need to be rolled back.

The third event occurs in the middle of the year, which is the revocation of the old key so that there's no residual trust in that old key.

I should note inside all of this that whilst this sounds incredibly technical, and it probably is, but inside of all of this is an overarching document which is the certificate practice statement which details how ICANN looks after that bunch of bits.

The only reason why the world should trust those bunch of bits is because ICANN is making a unilateral public commitment to manage the key in a certain way. That practice statement is, indeed, I believe, a document the board should read and thoroughly consider at all times because it is part of the reason why the world trusts you and the world trusts the management of the keying information that is at the heart of the security of the DNS system.

So when commitments are made in that practice statement, we'd certainly advocate to you that commitments made on behalf of all of ICANN -- and there is a certain responsibility of the board to ensure that it is both fully informed and responsible in terms of adhering to that practice statement. So I'd certainly commend that to you as being a critical part of your responsibilities as a board. And the staff then actually

understands what is required at the technical level, that the practice statement is a very key document. Thank you.

PATRIK FALTSTROM: Asha, please.

ASHA HEMRAJANI: Thank you, Patrik. Thank you, Geoff. That was very useful, indeed. I just wanted to ask if someone from staff, or David perhaps, could speak to the time lines and address some of the questions that Patrik had brought up earlier, or concerns rather. Thank you.

DAVID CONRAD: Sure. So we're aware of the time lines obviously within the design team recommendations. The challenge that we on staff are facing is, as you might be aware, there are a few things going on right now. In particular the folks who are responsible for key management are also the folks who happen to work in IANA. During the middle of the transition, their amount of available bandwidth to deal with the process changes necessary to modify the necessary scripts that are used to generate the keying material, stuff that is audited at every key ceremony, is somewhat limited.

So the challenge that we're facing right now is essentially a limitation on resources. And I guess the risk that we face is the longer that we delay rolling the KSK, the potentially larger the user base is of people who would be affected.

However, it is also the case that the longer we delay rolling the key, the more likely that the software that's going to be used to implement the DNS will support rolling the key in a more reasonable fashion and less likely to experience breakage.

This is the software both in terms of DNS software but also in terms of routing software and filtering software where we expect the problems to most likely show up due to large packet sizes being dropped left and right.

So right now we're trying to evaluate the best course of action given the limited resources that we have available. We have not settled upon a particular decision at this point in time about when we will initiate the process of rolling the key.

We have undertaken beginning the process of developing the communication plan. We've hired Adelman to help us with developing that plan. We have continued to develop the actual operational plans that will be done in conjunction with VeriSign. And depending on time frames, NTIA, the implementation plan will use as input the recommendations from the design team.

But we anticipate the implementation plan, the testing plan that we need to develop in order to minimize the risk of breakage, the backout plan should we discover the breakage is worse than we anticipated and we have to fall back, and the communication plan, we expect those to be done in the relatively near future. I don't have exact dates and times because that requires us to get a further grasp of the actual implementation requirements. So I hope that answers your question.

ASHA HEMRAJANI: Yes, thank you, David.

RAM MOHAN: Are there other -- Russ?

RUSS MUNDY: Thanks. And thanks, David. Russ Mundy here. I would like to speak a few more words about risk and the risk balance associated. Each activity has a given set of risks, and sometimes they're not always easily visible. And in the case of rolling of the root key, it is something that the longer it waits, the risks keep moving around and they keep shifting.

And at this point, it appears that the longer we wait and the more the growth of the use of DNSSEC happens, the greater the pressure is going to be to start also addressing algorithm rollover which is even more complex than root key rollover.

And so when we get to the point where we want to or need to do the algorithm rollover, it would be -- seems to me it would be much better if we were at least reasonably practiced in making the key rollover before we get to the algorithm rollover so we can take it in smaller steps.

And we know right now who most of the large validating resolvers are but not all. But the longer we wait, the bigger the number grows and the harder it becomes, especially when the new validators start to look for the new algorithm rather than the current.

DAVID CONRAD:

David Conrad in case this is being recorded. I don't know.

The risk -- the evaluation of the risk associated with a key rollover is, indeed, extremely challenging. For example, just a month ago, a couple weeks ago a bug was discovered in a library that's used in many software packages. And that bug had in its advisory recommendations -- or observations, perhaps, that if

you filtered the size of the response, then you would not be impacted by this bug.

That filtering of the length of the response would suggest that if people were to do that, then a key rollover would have a -- regardless of when it is done would have a very high failure rate for all of those resolvers that are so configured.

Over time, it's unclear to me -- and I can see arguments on both sides -- about whether doing the roll now or later has a greater or lesser risk. That really isn't the issue from my perspective at this point in time.

The issue that we face right now is, in my view, simply a lack of resources that we can throw at this particular problem. As I mentioned, the folks who are involved in the IANA transition at a very internalized level are also the ones who are involved in key management. We have a number of projects that are ongoing within IANA to deal with the transition.

We also have a number of projects within IANA that are aimed at improving the infrastructure to greater -- to facilitate more flexibility in the ability to do things like roll the key and manage the key ceremonies.

So while I definitely agree that risk is a significant issue, there are also some overriding factors here in my view that are related to the operation of the key management.

And with that, I'll give it to Chris.

PATRIK FALTSTROM: Chris, please.

CHRIS DISSPAIN: Good afternoon, everybody. Chris Disspain. I'm going to preface this by saying two things. One, what I'm about to say may be incredibly naive; and, secondly, I'm not even remotely technical.

It seems to me from a practical point of view that irrespective of when you actually roll the key, there's no harm in having a plan in place so that when you're ready to roll the key, the plans already there and you can do a risk assessment at that time.

So what I suppose is a question for David is: Are you saying that you don't have the bandwidth to create the plan right now so that at least we would have a plan ready for the rollover when we decide to push the button?

DAVID CONRAD: No, I'm sorry. We are actually engaged in developing the plan now. So it's not just one plan. It's a set of plans. We are actually in the process of developing those plans now.

We were waiting for the design team for some period of time. They finished their report, I believe, like November of last year. We had some internal resource limitations on my team that resulted in delays for which I apologize that it took so long to get the finalized design team plan completed. But it has -- as has been mentioned, it was released today. And that is the input document into the development of a number of the plans that we are developing.

PATRIK FALTSTROM: Thank you very much.

Please, Greg.

GREG AARON: Chris, Greg Aaron here. There are actually two components to plan for this. One is the purely technical plan which David and his team are working on, but there's also an outreach and communications component because we are going to break something somewhere.

And so SSAC had recommended as part of that plan we have to get out ahead of that problem and talk with the relevant communities so they know what's coming and can have time to prepare for it.

DAVID CONRAD: To be clear, we are -- as I mentioned, we hired Adelman to help us with the outreach plan.

RAM MOHAN: Thank you, David.

What I would like to do is go to the rest of the members here and after we're done with that, try to put a line under this item. So I see Danny in the queue. Is there anyone else? Danny.

DANNY McPHERSON: Danny McPherson, SSAC. So I just had a comment there is something else that's interdependent here as well, there is the ZSK key link size going from 1,024 bit and some presumed capability to factor that to a 2,048-bit key for the root signing key that VeriSign manages.

A plan has been communicated and coordinated with ICANN related to that, and we don't believe -- and VeriSign is certainly prepared to move forward with that. We don't believe that the

time lines would necessarily overlap with the KSK plan that's been put forth today to be done by the end of the year.

That said, there are some technical interdependencies that should be considered. But I think, in general, as an SSAC member, the care and feeding and maintenance of these activities is paramount to the security and stability of the infrastructure. And as part of the transition plan as NTIA stated on March 14th, security and stability was one of the tenets, that this not disrupt security and stability of the infrastructure.

And so I do believe this is extremely important. And that what Geoff conveyed a moment ago was extremely important.

One other thing I wanted to point out, which I would like to try and avoid in the future is, that many of the primitives associated with the name collision issue, for example, instrumentation of the infrastructure, broad outreach to relying parties of the infrastructure and potential impacted parties of failures are the same primitives that are required for the DNSSEC key rollover functions. And that work needs to exist regardless. And I think we certainly made leaps and bounds from the efforts that ICANN and the community has put in place there.

But we certainly need to work on the continued preparedness and communication to relying parties of the infrastructure. I think it's well understood what needs to happen. I'm not sure,

you know, what value a lot of other external engagement is. We kind of -- SSAC, I think, and the community kind of understand fairly well what needs to happen. It's just a matter of beginning the implementation, which I realize as well is the difficult part.

DAVID CONRAD:

I would just like to comment that I strongly agree with what Danny has said with regards to instrumenting the infrastructure. This is something that if we have that instrumentation now, it would help immensely in us understanding the potential implications of the key roll. Unfortunately, we don't.

RAM MOHAN:

Thank you, David.

Patrik?

PATRIK FALTSTROM:

Yes, thank you very much. I think that was a very good discussion. And, also, what I think -- people that have not been part of the discussions the last couple of days, now we understand how thankful I am for everyone that has been helped with moving this forward.

So from an SSAC perspective, as you heard, the first date in this report that was released is April 1st. It's really important from

SSAC's perspective to decide before April 1st what is to be done on April 1st or before that. So I have a question to you and the board. Have you had any time to think about what you're going to do to help and what we in SSAC can do to help to move this forward?

Understand, of course, this is something between main us and David. But, on the other hand, as we heard Geoff said, it involves all of us. So what can we do together between specifically now and 1st of April?

RAM MOHAN:

Bruce?

BRUCE TONKIN:

Thank you, Patrik. I think you have got our attention. The board's exchanged a few thousand messages in the last two minutes.

So I think now that you've got our attention, it's now our role to work with the CEO. In fact, we'll have a new CEO on the 1st of April. Or sorry, new (indiscernible).

[Laughter]

But -- but the CEO in place at that time will actually be Akram, thank you.

So I think just a general observation, I guess. And I was hearing David sort of talk about the challenges with the priorities. And as you know, we've had a large amount of the community busy sort of looking at how to reorganize ICANN. But at the same time, our fundamental mission is actually the security and stability of the identifier system. We have to execute on that. And so, you know, this really will be our -- one of our highest priorities. So I can assure you we'll talk to staff about this tomorrow and hopefully get back to SSAC fairly quickly as how it will relate to the timing.

PATRIK FALTSTROM: Thank you very much. And as I said, if there is -- we are -- as we are -- well, let me try again. I hope that you understand that by us pointing out the date 1st of April that is an indication to you that we are prepared to work really hard between now and then.

RAM MOHAN: Thank you, Patrik. I think that brings the first important topic to a close. Let's go to the second topic.

PATRIK FALTSTROM: Ben, yeah.

BEN BUTLER:

Okay, so this is Ben Butler, for the record. We wanted to take the opportunity to discuss the recent effort by ICANN to introduce key performance indicators, or KPI. There was a public comment period -- or a comment period recently and we submitted comments as part of the document SAC77. In the interest of time, we have some talking points here as to some of the thoughts that we submitted in that document. I think at a -- at the highest level our biggest comment is that the methodology and approach to the proposed KPIs is a bit backwards. The -- the metrics that were proposed seem to be based around collecting data that is already easily available and trying to derive meaning from those metrics whereas what would be much more meaningful to actually indicating the health of the domain name space would be to think about what it is we actually need to identify and then think about what metrics would actually get us to that point.

As some examples, we had recently published a document, SAC74, I believe, where we were looking at the registrant data protection and credential management life cycle. And there is a proposed KPI that you could use the number of reported breaches by registrars as an indicator of the level of trust in the - - consumer trust in the domain name space, and that -- that information is easily available because there's a certain number of breaches that are reported by registrars. But that doesn't

actually say what level of consumer trust there is. There are other resources potentially out there that would be better indicators, but there's also clearly a need to -- if we really want to get into what are the key performance indicators in the domain name space, there's some data that is either not currently being collected or not currently being shared that we would need to get from the registrar community, the registries, and so forth.

Greg Aaron submitted several comments as part of the comment period as well that we can go into, but again, they mostly center around we're approaching this kind of in a backwards fashion. And we're hoping that we can maybe encourage ICANN to take a step back and approach this from a more holistic view.

RAM MOHAN: Steve.

STEVE CROCKER: Thank you. I'm generally very empathetic with using a measure of complaints, what -- there is one peculiarity when you measure complaints. People stop complaining under two circumstances. One, when they're satisfied and the other when they've given up thinking that it's going to be helpful to complain. So I'm not

sure exactly -- you know, you have to guard against just using that as the metric, I think.

RAM MOHAN: Do you want to respond, Ben?

BEN BUTLER: Apparently what I wanted to do is knock over the water bottles. My apology.

GREG AARON: Greg Aaron here. So there were some proposed metrics that centered around complaints made to ICANN. And in some cases those may be useful, and in some cases the complaints don't measure what people thought that they were measuring. For example, the number of breach letters sent to registrars and registries does not actually tell us how many of them are compliant with their contracts because of the process that's used to get to those breach letters, for example. WHOIS was another place where the number of complaints was put forth as a metric to talk about accuracy and people's satisfaction with accuracy. We said -- or somebody said well, we actually have a WHOIS accuracy measurement program. Let's use metrics from that. That will actually tell us some facts and figures that will tell us how we're doing.

So we wanted to use this opportunity to educate about especially some of the security and stability-related issues and how to measure them effectively so they would -- they would tell us all about how ICANN and the ecosystem is performing.

RAM MOHAN: Thank you. I have Cherine. Cherine, Erika, Cyrus in the queue. Cherine.

CHERINE CHALABY: So I'm very sympathetic to the point that you make because I want to make sure that we understood it. So you're saying by the word "backward" is we are collecting data and then deciding what to do with it as opposed to identify what the issue you want to collect data for and then go ahead and collect the data to substantiate or negate it; is that what you're saying?

BEN BUTLER: Essentially, yes. And by doing it that way, sometimes you create a mismatch of what you think you're actually saying.

CHERINE CHALABY: It would be interesting to get -- I don't know if Akram is here or Cyrus -- to get a -- to comment on that. Okay. That would be quite a good -- okay, thank you for that observation.

RAM MOHAN: Erika.

ERIKA MANN: Yeah. It's similar to what Cherine -- what Cherine is asking. I read actually what you wrote, and you quote Greg Aaron. And you say in other quotas because it becomes then maybe clearer. You said Greg observes that some of the proposed KPIs are crafted around data that is currently available that makes them cost effective to collect but it does not mean the data is always fit for a designated purpose. In some cases ICANN may need to develop new sources of data.

Now, I agree with you. This is always a problem. If you want to analyze data, you need to understand what you actually want to analyze to raise the right question and then maybe to have access to data which you don't always have access to. So what is actually missing? When I -- I read this quite carefully, but what I would love to see from you, I think would help us all, just to have a simple overview what kind of questions -- what kind of access to data actually you want to have? Maybe I missed the point, but it would be nice to get this maybe in a simpler version from you.

RAM MOHAN: Ben.

BEN BUTLER: So -- thank you. There are some specific examples pointed out in there, and I'll point to the breach notice that I mentioned earlier. Under the 2013 RAA the registrars have to report breaches, but that's as far as the requirement goes. As part of SAC74, what we were recommending is that that -- that breach reporting needs to be analyzed again. It would be useful when as a community we had access to the number of -- not just the number of breaches but what type of breach was it, how many users were affected, did it have to do with credential management. We can do that without, you know, getting into a -- you know, a registrar shaming or registry shaming situation, but more detail would actually give us a much better indication of the level of health in that domain name space. And that -- just as an example of how the methodology might require new data that we don't currently have access to.

RAM MOHAN: Thank you, Ben. Patrik, you wanted a quick intervention on the data point.

PATRIK FALTSTROM: Yes. When we say other data or that is not available, that doesn't mean that the total set of data increases. It might be the case there are lots of data collected that is not needed. So you need this evaluation to collect exactly what you need and not more.

Mark and then I see Cyrus would like to -- want to enter in. Mark, you first.

MARK SEIDEN: Some of us who worked on the registrant protection question in the credential document, SAC74, believe that it's a fundamental principle that when people's credentials are compromised they should find out about it somehow, and in the U.S. it's quite common that breach notifications are sent to such people. Although ICANN has data on registrar breaches reported, it doesn't publish those on a detail basis. So my personal belief is that it should be required to collect and publish that data for the purposes of protecting the registrants.

RAM MOHAN: Cyrus, you're the last in the queue, and I'm just mindful of time. We have about 9 minutes left in this session. So after Cyrus is done with this topic we'll move to the third which is a briefing.

CYRUS NAMAZI:

Thank you, Ram. Cyrus Namazi from ICANN GDD. Perhaps it would help everyone in the room if I explain what this initiative is about so we're all on the same page. Some people may not know.

So this is an exercise in an initiative for constructing a dashboard to analyze and track the health and diversity of the gTLD marketplace. That's the key objective behind it. So to that end, on the staff side we composed a paper. In it we put in a set of proposed ideas and criterias. And I underline the word "proposed" here because we really were looking to the community, the experts, yourselves on the SSAC side and others, to really come help us construct what it is that we should be tracking to indicate what it means to be measuring the health of the domain name marketplace, for instance, and what are the metrics and gauges that we need to go collect data for. Some of them, as you said, available, some of them are readily available and some of them not. And we posted it for public comment in late last year.

The depth and breadth of responses that were received has frankly totally surprised me. The level of enthusiasm has been great. We received over 30 public comments, one of them, of course, from SSAC. Incredibly useful information.

None of what we put in our proposed paper was supposed to mean that these are cast in concrete. They were just proposed topics for -- to facilitate discussion. And I'm glad it actually has helped to do that.

The SSAC input has been incredibly helpful actually. So since the end of January, when the public comment period closed, the staff has taken everybody's inputs. We've incorporated them into our -- into the paper, and soon will be posting it back for the public to see. There is now a group of 30 volunteers, as a result of this initiative, that have volunteered to be in an advisory board to work with staff to define what it means to say the health of the gTLD marketplace and then like you said work it back to see what it is that we need to be measuring, tracking, the type of data that we need to collect.

I'm actually quite optimistic, and I'm very grateful for the community for the energy they've put into it because the knowledge base and the vision of it needs to come from you people who are experts in their respective fields. And rest assured that there's nothing in there that is really pre-defined by the staff. It needs to be done by you. It's an iterative process, so it's going to continue to be improved and fine-tuned and sort of get to the next stage of it. But I hope that helps.

RAM MOHAN: Patrik.

PATRIK FALTSTROM: Thank you very much. So next last topic, and this is just information for ICANN board, one of these that we just started work on. Jim.

JIM GALVIN: Thank you, Patrik, I'm Jim Galvin, vice chair of the SSAC and in this case I'm co-chair of this particular work party in SSAC with Lyman Chapin sitting here on my left. I believe you have another slide queued up with a diagram on it. If you could move to that slide.

So most of the board will recall that we gave a briefing at the last ICANN meeting where we were highlighting for the board an issue that we believe is of some importance and some significance. And so this is an update from us on this particular topic about namespace. Our goal here is to keep you aware and remind you, in essence, that we believe this topic is important.

What we have here is a diagram which is now forming the basis of our discussions which we believe reflects this problem space. And I want to just take a few minutes to make some bullets points here about this diagram that we hope will explain the

overall problem space that we're dealing with and looking into with our work party.

So there are three things to understand from this diagram. The first is that this is just a snapshot of some of the subsets of all possible TLD strings that exist today. So, for example, the IETF has a registry of special use domain names, the Applicant Guidebook had its own list of reserved TLD names, right? There is a list of TLD names that are in the root zone, and each of these represent subsets of particular lists of TLD names.

The second thing to understand about this diagram is that each of these subsets have their own inclusion criteria. In some cases this is fairly well-defined, so we can consider the TLD labels in the root zone. I think for the most part we would agree that there's a fairly good definition of what can and cannot get into the root zone. There are some edge cases to consider, but for the most part that's fairly well-defined.

The third thing to understand about this diagram is that there are rules that determine whether a string may be moved into or out of any one of these subsets. And here again, there are cases where this is fairly well-defined, the TLD labels in the root zone and some of the other lists, and somewhat loosely -- more loosely defined in some of the other lists.

The other thing to keep in mind is, as I said above in the first point, this is just a snapshot. So one of the things to consider is, this is not necessarily all the possible lists of labels that could be valid to be a TLD string. There may be other organizations, other venues, other bodies that have their own lists for their own purposes and their own reasons, and it's important to keep that in mind.

And that brings us to the three main questions that we are using as the basis for our discussions. We want to make you aware of these also, so that you can have some time to think about them. If you'd like some more details about them, there's certainly any of us that you could speak to and would help inform, you know, your discussions about this topic.

The first is, how are the rules that determine membership in any one of these subsets defined? Since the lists will be coming from different sources, those different sources will have their own ideas about what goes on their list and what doesn't. And that's important to understand that some of these are better defined than others.

A second question is, what are the rules for moving a string into or out of a subset that is there? And again, in some cases, whether or not you can be a member may or may not be well-defined and whether or not you can become a member or be

removed from membership may or may not be well-defined. It's important to keep those things in mind.

The last question is probably the most significant question, and this is -- it is this last question which is why we believe this issue is of some significance, especially in the ICANN community and what we would most like emphasized for you to keep in mind. And that is, what does the intersection of any two or more of these subsets mean? So what -- what does it mean when a name is on -- or a string is on one of these lists and not on another? What does it mean if a string is on both of these lists? And what happens as in the example if you look at the boxes up here you see at least three of the boxes that don't have any overlap. This is, in fact, a traditional -- intended to represent a traditional Venn Diagram, if you will. So TLD labels in the root zone. You have a list of names, special use domain names like .ONION as an example. You have a list of reserve TLD labels in the Applicant Guidebook, for example, ICANN. That's a case where the intersection is in fact the null set or empty. There's nothing there. You want that to be the case. Probably in all of these cases. All right? But is that meaning well understood, is that meaning documented? Are the respective bodies that create and manage their own lists talking to each other and communicating and aware of the fact that they have to respect each other's lists?

So that's really the last question in all of this, and this is just our update to you. And it's primarily this diagram which we hope actually very tangibly and as a practical matter explains to you what this problem space is and why we think it's important. Thank you.

RAM MOHAN: Steve.

STEVE CROCKER: Thank you, Jim. It's very -- very helpful, very clear. So I've followed streams of messages on this for a while. The special use names seem to be coming out of a tradition in not necessarily the IETF per se but in that general vicinity of first we'll build it and use it and then we'll let people have a discussion about whether we'll register it.

And so to have a discussion about how to coordinate these things presumes that there is an agreement or an implicit agreement that there ought to be some coordination, and I detect in at least some portion of the community a pretty strong resistance to the very notion that we'll coordinate anything, we'll just go do what we want and then don't have to be bound by any rules.

I'm putting a bit of spin on it, perhaps, but you understand what I'm saying.

RAM MOHAN: Thanks, Steve.

Jim?

JIM GALVIN: Oh. Yeah. Just to respond to that, I think the response to that is to consider those free-floating names at the bottom of the diagram: home, corp, and mail.

I mean, it is true to some extent that these bodies could exist independently and certainly have their own reserved names, their own reserved lists, but name collisions is a topic which we will all remember from a couple of years ago and we are still living with.

The problem that you have is, even though different bodies may have their own lists, the use of those names leak into other circumstances, and that's why coordination is necessary. Either that or you have technological issues that you need to deal with. And that is really what has created the existence of this problem, or made it visible to more people. Thank you.

RAM MOHAN: Thank you, Jim. I think the -- from -- to the board, the -- a couple of messages.

One is, watch this space. This is important stuff.

And second, I think on behalf of the board, we'd really express our gratitude that you're watching this space and you're helping explain the differences and the importance of keeping track of these differences.

So in many ways, from the board, we look to you and to us, if you will, in SSAC to help provide guidance and the next steps forward.

So with that, I want to thank the SSAC for coming and for meeting with us, and appreciate all that you have done, and I'll give the last word to you, Patrik.

PATRIK FALTSTROM: Yes. I would like to also thank the ICANN board for having this meeting, as I opened the meeting with, saying that we really, really look forward to these meetings with the board for every SSAC meeting -- at every ICANN meeting, and we look forward to continue working with you and the next ICANN meeting, of course. Thank you.

RAM MOHAN: Thank you. This session is adjourned.

STEVE CROCKER: Thank you.
[Applause]

[END OF TRANSCRIPTION]