Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

HSTLD Advisory Group Teleconference on RFI

23 November 2010

Coordinator: Welcome and thank you for standing by. At this time all participants do have open lines. Today's conference is being recorded. If you have any objections you may disconnect at this time.

I'd like to introduce your host for today's conference, Mr. Craig Schwartz. Sir, you may begin.

Craig Schwartz: Thanks, Operator. And thanks to everyone who has signed up to participate in this conference call today about the High Security Zone Verification Program being developed through the HSTLD Advisory Group and ICANN.

My name is Craig Schwartz and I'm one of the two ICANN staff supporting the Advisory Group through their work. The other is Dave Piscitello and I don't see that Dave has joined the call yet, but Dave is Senior Security Technologist at ICANN.

I'd also like to take this opportunity to introduce the Chair of the group which is Mr. Michael Palage and the other gentleman who will be helping co-lead the call today is Mr. Paul Smocer from the Financial Services Roundtable.

What I'd like to do before turning the call over to our Chair, Michael Palage, is to do a roll call. And what I'll do is I'm going to read directly from the list of people that are signed into the bridge. I know some of the firms have indicated that they'll have other people joining them. So when we get - when I get through the entire list if we have other folks on the line if you could identify yourself and your company name that would be great.

So on the line right now we have, (Spencer Rossner) from PricewaterhouseCoopers. We have Steve DelBianco from NetChoice. We have Adam Palmer from Symantec. We've got Kathryn Holt from Ernst & Young. We've got (Raymond), and (Raymond), I'm going to mess up your last name, but (Van Krimpen) from Deloitte.

(Raymond Van Krimpen): You got it.

Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

Craig Schwartz: Thank you. From Deloitte. We've got Mikey O'Connor from the O'Connor Group and Mikey is one of the Advisory Group members. You've got (Myra Talossa) from Ernst & Young. We've got Mark Lundin from KPMG. We've got John McElwaine from Nelson Mullins. John is also a member of the Advisory Group.

We've got Tim Davis from Deloitte & Touche. We've got Paul Smocer from the Financial Services Roundtable. Paul is an Advisory Group member and co-lead on the case. Paul. We've got Michael Palage from Pharos Global and Michael is the Chair of this Advisory Group.

We've got Ken Michaels from PricewaterhouseCoopers. We've got Kevin Anderson from Grant Thornton. And we've got Lynn Goodendorf from Good Security Consulting.

If there are other folks on the line today that I didn't call out by name, would you please speak up and identify yourself now?

Is Tim Davis?

Tim Davis: Yes, Craig, I'm here.

Craig Schwartz: Tim, are any of the colleagues that you indicated, Donald - I know (Raymond) is on the line, but Donald Sheehy, Jan Carstens and (Vicky Folen), is there any of those folks with us?

Tim Davis: No, they're not. I got a note from Jan saying that he wasn't able to make it, and I think that's the same for Don Sheehy.

Craig Schwartz: Okay, and then Kate, from Ernst & Young, you indicated that Pete Jansen and Mark Sogomian...

Kathryn Holt: Sogomian.

Craig Schwartz: ...Sogomian.

Kathryn Holt: Mark was unable to make it and Pete may be a minute or so late.

Craig Schwartz: Okay. Have I missed anyone else on the - on the phone bridge today? Okay, hearing none I will turn the phone over to Michael Palage and to Paul Smocer. Michael?

Michael Palage: Thank you, Craig. And again, I'd like to thank everyone for participating in this call today, particularly those people that may be respondents to the RFI because that will be an important part of this group's fact-based decision making process. So again, I thank you.

What I'd like to do is just briefly provide sort of a two minute high level overview of where the group started, where we're at and where we're going. And I would first like to begin with sort of some of the consensus points that we have reached or consensus points that we've reached and also identify those points in which there are still diversions or differences of opinion. Because I think that's also something that is important for RFI respondents to appreciate.

So as far as the consensus, there definitely is consensus about doing something to enhance the security of, if you will, TLDs, not just new TLDs, but existing TLDs. Now one of the elements that we've done which you I think have looked at in the reports that we provide, is to come up with a set of control elements.

And as I said, within the group there has been I would say general support for the control elements that appear in our reports. Where there is some diversion within the group is how those control elements might be used as part of an HSTLD program.

And two of the concepts that have been discussed, one is a certification program along the lines of say an ISO certification. We've talked about potential uses of a (seal), there's also been the concept of a report card that perhaps is less onerous but would still involve some type of validation by a third-party.

So I think that that is important to get out there at the beginning these points of consensus as well as diversion. And one of the other points I think that some community - some Advisory Group members have expressed and which we would really value hearing from you today is how this program might be able to go down the value chain within the domain name system.

Most of our control elements have primarily focused at the registry level. We have talked about how it might apply to the registrar and perhaps the end registrant level. So any experiences that the people on this call might have with those types of value chain propositions would be very beneficial to us as a group.

So again, as a Chair I have primarily been the, if you will, the process master, making sure that the trains are always running on time. To make the best use of your valuable time on this call, I've asked the help of Paul Smocer who is more perhaps a subject matter expert in this area to perhaps lead us through the call. And I will be able to coordinate any types of cues or interactions from other participants.

So at this time, unless there's any questions or comments, I'm going to turn this over to Paul and allow him to start, if you will, driving through some questions and engaging in some information sharing and exchange of data points. Okay, Paul?

Paul Smocer: Okay.

Michael Palage: It's - you have the (floor).

Paul Smocer: All right, thanks. Again, this is Paul Smocer and as Craig mentioned earlier in the call I had been a member of the Advisory Group. I should probably upfront note that in relation to the comments Mike made about perhaps some diversity in the group, obviously as - being here as a representative of financial services industry this is a very important program to us with regard to helping to assure that any new domains that relate to financial services get the best level of security possible.

So I'll (drive) that little statement ahead of time so you have an idea of a little bit of where I would be coming from in this conversation.

What we'd like to do first, if we could, we had provided you with a series of answers to the questions that had been raised by very respondents to the RFIs. What we tried to do was to put everyone's questions in one document. So you may not have asked, maybe one of your colleagues that has left the firm had asked the question, but we thought that all of the questions deserved to be presented to you all so that you could see our responses.

So let me start first with a general invitation with regard to any follow-up you have on our answers to any of the questions. So if you have any follow-up questions to how we answered or where the vision is this is your opportunity to go ahead and present those to us.

Ken Michaels: Hi, it's Ken Michaels, I'll jump in. One of the questions we had was around basically the sponsorship for the program. I was previously thinking that ICANN would actually administer the program themselves and handle the certification, management, etcetera.

But it looks like you're proposing another third-party or body or governing body basically administer the program. Any further thoughts on who that would specifically be? I think that would be one of the biggest challenges we have, getting somebody to actually own the whole program.

Michael Palage: Paul, do you want to take that and then perhaps I could - you want to take that first and then I could perhaps chime in with sort of where I think the group has been over the last year?

Paul Smocer: Sure. And again anybody from the Advisory Group who might want to feel the need to correct what I'm about to say, please feel free to jump in. You know, I think when we think about the program, we tend to think of it in two major component pieces.

One is the standards themselves and then one is - well, maybe three component pieces - the standards themselves the, for lack of a better term, validation process to assure that someone is conforming to the standards and then the third piece is ongoing development and, you know, modifications, changes, etcetera that may need to be made over time.

And I think if you think about those three components, in answer to your question, I think as a group, we feel that we have gotten the standards pretty much to the point where we are satisfied with them in the initial iteration.

I think as a group, we feel that the HSTLD Advisory Group will continue as a living body going forward and would likely bear primary responsibility for any future changes to the standards, etcetera.

And I think it would be safe to say that ICANN will remain supportive of the existence of the Advisory Group and the work they're doing in terms of standard setting.

I think where the confusion may be coming in is that second component around the "validation" process where ICANN has essentially said that they would prefer not to host that process, be a part of that process or, you know, even in a way have their name associated in the sense of some sort of seal of approval with that process.

So that, you know, part of the conversation we want to have with you guys today as well, is to talk about alternatives if in fact ICANN continues down that route, if it's important for you all to know that there are discussions underway with regard to what will finally be the role of ICANN in that validation and the seal of approval concept space.

And those are still open discussions, so we don't know where they're going to resolve themselves, but I guess answering your question, in that space, we might be looking for or consider an alternative in which someone oversees the validation program and is the entity that coordinates that program and issues whatever seal of approval - and again, forgive the nomenclature, but whatever seal of approval might end up showing up on the internet to indicate that, you know, you're in a domain that has met the standards for HSTLD.

So that's really the component place where I think there's still some open questions and where we would likely, at least at this point, be seeking alternatives for someone to run that.

Obviously, whoever that is, we would expect would also assist the Advisory Group, the HSTLD Advisory Group going forward in the standard-setting process as well, but if you think about where we are today from an ICANN perspective, it's more around the validation program and public-facing awareness of the validation of a domain as being in the high security space.

Ken Michaels: Yes, we do things...

Paul Smocer: Mike, would you (unintelligible)?

Ken Michaels: That group - sorry to interrupt - that group, would that be - whatever group that is or whatever consortium or body, would that be funded by ICANN? Or are you expecting like, a third-party to basically assume that and then take some type of fee to fund that organization from everyone that gets the HSTLD or maybe unknown?

Paul Smocer: I think it's probably more in the unknown. I think given where we are with the questions around the validation program, we would certainly entertain a model in which whoever is coordinating it does it, you know, on a fee-based (service). So, you know, I'll kind of hold my answer there and let Mike jump in if he wants to.

Michael Palage: Yes, thank you, Paul. So while I think Paul's answer is perhaps consistent with the most recent Board resolution on how they would like to distance themselves or provide a buffer in connection with this process, I perhaps have a little different personal viewpoint that I would like to just share.

I find for those people that may be familiar with ICANN, I see this as being somewhat analogous to the UDRP process. Now, the UDRP was a policy that was developed internally by ICANN and its still one that is maintained internally and can be edited within the ICANN structure.

However, what ICANN does is, they actually approve ICANN-accredited dispute provides, which then administer this. So for example, ICANN has approved NAF, they have approved WIPO, they have approved the check arbitration court.

So they have approved these entities to administer this policy, right? So I guess my view, again, personal viewpoint here, would be that ICANN would retain ownership or control over the criteria and that as far as maintaining control of that, individual members would be able to participate.

So just to give you a rough data point here, both WIPO and NAF participate within the intellectual property constituency, so, you know, if a Deloitte or if a KPMG wanted to participate, they would be able to share their experiences in proposing changes, edits or evolutions into the control criteria.

But those control criteria would be within ICANN's remit and then ICANN would accredit, you know, entities such as a Grant Thornton, a Deloitte, a PricewaterhouseCoopers, to administer these.

And much like the UDRP, it is up to that provider to set the fees that it sees right. Fees are not mandated in connection with the UDRP. That is up to the market to set those fees.

So I think that is another potential implementation path that perhaps is a little less costly and does not require, if you will, that funding of a separate organization to administer the process. So I think that is another model that should be potentially put out, put on the table for consideration. So I just wanted to put that out there, Paul.

Craig Schwartz: And Mike, this is Craig, and in terms of talking about potential models, it's certainly within the final report that the HSTLD Advisory Group is going to issue sometime in late January or early February, that model could be something that's included in that report.

Michael Palage: Well, we will discuss models and hopefully we will have consensus within the group on those models and if we don't have consensus, we will list majority or minority viewpoints, so that, but yes, this is something that will be contained in the final report.

Paul Smocer: So does that - I think that was Michael that answered the original question, I mean...

Ken Michaels: Yes, that's great.

Paul Smocer: Did those two models help in your understanding and perhaps if you could give any feedback on which might be more implementable based upon your experience in this - these types of programs, if any?

Ken Michaels: Yes, very helpful. I think the ownership of that administration, that's where the nuts and bolts of this program will be implemented. Some sort of ICANN sponsorship of that, which should have a global perception and a global footprint would, I think, be a critical, critical component of this.

I don't think there'll be a third-party who's just willing to necessarily invest in this without a clear ROI. So it’ll be tough to find a, you know, an organization non-profit or other that would help administer it. So I think your participation in that whether it’s certifying a creditors or other or violation monitoring I think is really a critical component.

Without that I don’t know how the actual implementation would really take off so I think that would be great if you could do that.

Craig Schwartz: And put it this way -- thank you Michael -- perhaps if some of the other and for those people that are not used to my chair qualities, I generally try to pull teeth.

So if I could perhaps just going down the line, could the other potential respondents to this perhaps offer their opinion?

Tim Davis: Well Michael it’s Tim Davis with Deloitte. I’ll jump in...

Craig Schwartz: Thanks Tim.

Tim Davis: ...and give you my perspective. I do think that the model that you described is very consistent with how other standard fitting organizations also administer their role in terms of the standard panel so I think effectively mitigate the level of risk that they have in terms of being standard sitters.

I would tell you in most common practice when you’re in these sort of assurance standard type scenarios, the entity that’s applying for the validation is the entity that really, you know, owns and is responsible for the majority of the legal risk if there is any for non-compliance because they obviously have the responsibility ownership and are most familiar with their level of compliance.

And the way that these programs are increasingly run now is the entity applying for certification will actually make an assertion as to whether or not they’re in compliance.

And that’ll be based on some self-assessment. There’ll be a third party that comes in and basically opines on that assessment as to whether or not they agree with the entities management opinion.

And that way it clearly puts the management of the registry or the registrar on the hook first and foremost for, you know, taking a position on whether or not they comply.

You would then have, you know, an independent auditor come in and say if they agree or disagree.

Now I guess the question for ICANN is the level of role that they want to play in terms of them either hosting a scorecard. I know there's been some discussion about that.

It wasn't really clear to me the response you gave on Number 4 about a seal. I'm not quite sure how a third party would manage a seal. I think it kind of goes back to the previous question.

If there is going to be a seal program I think it is going to have to be sponsored and run by ICANN. But, you know, there's a whole sort of I think separate set of issues around seal programs because independent auditors issue reports typically at a point in time and it covers a backward looking period as opposed to a seal which is sitting out there in real-time.

And obviously as facts and circumstances change, the seal in terms of what it represents may not be a valid representation of what's happening at the entity so many other issues there.

And I won't go on too long, but I'll just give you I think four founding thoughts that I had that I think underpin a lot of the issues that the Advisory Group's been dealing with in terms of how we go forward.

And those four issues are I think ICANN needs to decide on the level of specificity that it wants in this program.

And if you want to go with an existing security certification program and that's going to be suitable, that's fine. And some of those have seals, some of them don't.

But if you think that what's required here is specific enough to TLDs and the DNS I think you're not going to be able to point to another third party seal. I think it's going to have to be an ICANN custom seal that's generated. So that'll be one.

Two I think would be the level of assurance you're looking for. There's all sorts of levels of assurance all the way from some on the end of almost a selfcertification with some monitoring like trustee, what they do with privacy all the way across to a high assurance model where you have an independent auditor coming in and performing an examination over a period of time.

So I think that's going to drive, you know, who ends up being the validated participant in this program. And I think a mixture of those doesn't really work unless you have tears, you know, say an entry level certification and maybe a higher level certification.

Three would be I think the level of consistency that you want around the world. And by consistency it would be both consistency of the approach, the qualifications of the validators and the consistency of the results.

You know, if someone gets approved in country Y that kind of meets the same thing as them being approved in country Z.

So the level of consistency I think will dictate the level of ICANN's involvement in looking at the results and then making a determination on the suitability of the validator in terms of the approach, the qualifications and then obviously whether or not the result is suitable, you know, as possibly recommended by the auditor.

And then fourth and finally was just access. And what I mean by access is, you know, in terms of how you design the program, how important is it that there be international access to the program either on behalf of validators?

And so, you know, if you're in a particular country and you might be say a chartered (a country) organization, you know, are we going to set this thing up in such a way that an organization like that can participate as a validator?

And then also obviously access to registries and registrants around the world. And if you set it against say, let's say a particular US standard, I mean they may have no way of hiring an auditor against which they could apply something against a US standard from another country.

So hopefully that's helpful Michael. That was just some sort of top of mind sort of thoughts I think that are sort of friendly principles for watching these countries as you go forward.

Michael Palage: Tim, thank you very much. And as I said, I'm going to just again step back and let Paul try to steer the rest of this.

There was just a little bit of quiet there and I just wanted to spark some things. So again, thank you. So Paul, I'll again defer to you here to lead the way.

Paul Smocer: No trouble (Mike). Actually I'd like to hear if there are others who would want to opine on the question that (Mike) asked. I think that the information we've gotten so far is actually very helpful for us.

So is there anyone else of the respondent group who would like to step in?

Okay, well I'm hearing a lot of silence there. So again, you know, I think that as we walk through the questions our answers probably reflect generally the conversation we've been having here that there are still some open items that we need to resolve, not the least of which relates to the ongoing role of ICANN in the process.

But again, looking to see if, you know, there are any outstanding questions that you have based on what we answered. We've gotten the one so far so I don't want to cut anybody off.

Well then we did - well I'll take that as a veiled complement that we did such an excellent job in answering the questions thanks primarily to Craig pulling it altogether in the group for - the Advisory Group for refining the answers as we went along.

(Mike) or Craig, do you have anything else that you wanted to bring up while this group is on the call?

Michael Palage: Yes, thanks Paul. I guess what I'd like to do here is one of the issues that we are struggling with with value chain of proposition and I think Tim was talking about this on the scope of how broad this program will be made available on an international basis.

Most of our work I think as the group could see has been primarily focused at the registry level. We have touched just briefly on what could be done at the registrar as well as the registrant level.

And one of the reasons we were hesitant of going down that far was the potential cost. So I was wondering if what would really would be helpful to the group I think would be any shared experiences from the accountancy firms on the end factorial complexity of going down that level and what could be done to, you know, perhaps if you will get maximum value or maximal protection with, you know, if you will, a reasonable investment of cost.

Because again, just a reminder, we were looking at the viability of this program. And obviously what it costs to do this or implement this is a factor that needs to be considered. So that would really be helpful.

So if perhaps, you know, Michael or Tim or anyone else could share their experiences, that would really be helpful to the group.

Tim Davis: Michael it's Tim. I can start out. I think there are a couple of factors that would drive cost, not least of which I think the four sort of founding issues that I started out with, clearly the level of specificity in the criteria that you end up with at the end of the day.

And the extent, the other thing is obviously is some sort of bifurcation in terms of which of these issues you think are going to be applicable to registries versus registrars.

But that being said, you know, to give you a sort of a, one of the frames of reference that I think the auditing profession uses in this type of value chain example is the SAS 70 or what is going to be called SSA 16 reporting of where an auditor comes in to provide assurance and controls to another user auditor around controls at a third party that may impact their other auditors opining on the financial statements.

So, you know, one example is Company A uses Company B to process their payroll. So that Company B's who operates the payroll engages an audit firm to come in and test those controls that are relevant to Company's A financial statements.

So in that situation when the auditor at the payroll processor goes in, they would typically record what are called user control considerations in addition to the controls at the payroll processing organization that any user of that service would have to contemplate in terms of achieving the control objectives of all of the criteria that's laid out in the opinion.

And just to give you one simple - a simple example would be if you're looking at logical access security control and there's a service that involves, you know, the user organization having to log into the service, the extent to which and how they protect those passwords is fundamental to the security of their overall system. So that passive protection would be called out of the user control consideration.

So there may be a similar model that works here with the registries and the registrars where and they each have a codependency on each other for different aspects of providing a secure service.

And if the auditor were to go in to the registry or the registrar it could call out those aspects on which it's reliant on the other members in the value chain.

And that way as a registrant just trying to understand, you know, what's the various, you know, where both, you know, organizations I'm getting involved with here and what is their respective compliance with the HSTLD criteria you would - you could actually put these reports side by side and actually understand the extent to which each other satisfies the aspects that they rely on each other for.

It is obviously then, you know, the downside is it's reliant on the user to pull it all together as opposed to, you know, some central knitting of it all together which I guess is possible.

But that's just one example of how it works today, you know, and in the - in the CPA world.

Michael Palage: Well put it this way Tim, thank you very much. That was very helpful. And that was - it was constructive for me because one of the things that I appoint it to over the course of the last year are some of the reports that ICANN has issued from the security and stability, the (S act) regarding some of the, if you will, security threats at the registrar level in the value chain of trusts there.

So I think some of those points there that you've proposed provide a potential platform or a path forward that is scalable. So thank you.

Kevin, you've been kind of quiet there. Is there any comments or questions or other contributions to what you've read and what you've heard so far today?

Kevin Anderson: No. I think the reason for being quiet is my colleagues at the other firms are doing such a good job of covering the high level issues.

Michael Palage: Okay, excellent, excellent. And Kate from Ernst & Young, do you want to contribute anything?

Kathryn Holt: No, I think we - we've got a similar opinion as to those things that have already been said.

Michael Palage: Okay so - and again, one of the things again is important for us as a group is -- and I just want to echo this -- so Kevin and Kate, everything that you have heard collectively perhaps expressed by Tim and (Mike), there's no disagreement with anything that you've heard that there is perhaps consensus among the firms to these broader points because I just want to make sure that when we do try to summarize this that we're getting it right so all right?

Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

Okay, I think that's about it from my standpoint. Is there anyone else - again I'd like to open this up. Anyone else on the call that would like to contribute?

You know, Steve I know you had raised some questions. Do - would you like to raise your question here now to the group? Or I - you were concerned about how this may improperly set the bar low for registry operators.

Steve DelBianco: (Mike) the last four questions that you guys responded to where the ones that I submitted as an individual.

And I'm keenly listening to today's call because the business constituency is trying to put together comments in the guidebook.

And I have to confess that one of my confusions is to the extent to which the momentum achieved by the HSTLD Advisory Group would worm its way into the guidebook, you know, in particular Question 35.

And so I'm focusing tightly on that just trying to get guidebook questions in. And that answer may impact the way the program moves ahead.

So I don't feel the need to go through my questions and what I thought were the thoughtful answers that you guys provided. I appreciate that.

But I did want to ask about the guidebook interactions. Thanks (Mike).

Michael Palage: Okay, thank you Steve. Let's see, Adam, you're on the call. Any contributions or interventions?

Craig Schwartz: Yes I think - hey (Mike) it's Craig. I think Adam, looks like Adam disconnected at some point though I'm not clear when.

Michael Palage: Okay.

Paul Smocer: Hey (Mike)?

Michael Palage: Yes?

Paul Smocer: (Mike), this is Paul. While we do have the group on the line, I have an additional question if people would be willing to share their thoughts as well.

When I look at some of these programs (unintelligible) security or reliability and I'm thinking of one that has three initials and starts with a P and applies to the credit card world, you know, there is always this struggle between how specific you get with the standards and how effective that specificity is in trying to essentially prevent the core issues that you're trying to prevent or put a more positive way, perhaps making the world more secure.

So I'm kind of curious as - if anybody has any advice to the group. This is off the subject of the validation process more into the standards, but any thought on how much specific good, you know, how we should be perhaps more general than specific?

And I guess going back to the validation, how much the specificity of a lack thereof effects your ability to validate someone when you do go out and take a look at them?

Tim Davis: Yes Michael it's Tim Davis at Deloitte. So I can offer you my perspective on that. And that is, you know, as you've pointed out, I mean the program that you referenced is highly specific.

There is the ISO-27001 standard which is not specific at all. It really just talks about sort of broad issues and leaves a lot of room for interpretation.

And I think it goes back to Item 1 that I started with which is in developing the criteria, if there is something specific that applies to securing the TLD, the DNS root -- whatever it might be -- that applies here that's not going to apply in general sort of systems, that I think you have to call out.

Outside of that I would say it's important to leave some wiggle room for interpretation. You don't want to get overly specific cause then you end up with, you know, just basically frustrating the entire system and the respondents that are trying to certify themselves against the standard.

But to the extent that you leave it open and really talk about principles as opposed to rules, the more you're on that principle end of that spectrum, I think the more careful you want to be in terms of the qualifications of the organizations that are doing the validation.

And so that would be the rule of thumb. The more open ended you are, you more careful you want to be about the qualifications.

The more specific you are, you know, you have less of a need to, you know, approve suitably qualified validators.

Michael Palage: So that would suggest and if we're more general than what's more important is somebody with the expertise and intellect to properly interpret what we're saying and validate it versus more of a - for lack of a better of a term, a checklist (depart) kind of scenario?

Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

Tim Davis: Correct.

Michael Palage: Okay great. Thanks. Anyone else?

Craig Schwartz: So Paul, perhaps what we could do here is we do have a - we're within the time limits. In the call we have (Lynn), Mikey, Jonathan and John who are also Advisory Committee members who have been shall we say stalwarts in the work of this group over the last year.

So what I'd like to do Paul is perhaps if you could take some questions from them and see if there's any interaction with the people on this call that I think would be a constructive use of time.

Paul Smocer: Thanks. That's actually where I was going to go next -- appreciate it.

So from the Advisory Group members who are on the call, you've been listening patiently. Do you have any questions or any observations with regard to what's been said so far?

John McElwaine: Paul this is John McElwaine. I'd like to get in the queue. I'm sure there might be some others.

Mikey O'Connor: Yes Mikey here I'll get in too.

Lynn Goodendorf: Yes, this is Lynn Goodendorf.

Paul Smocer: Okay. All right, John, why don't you go ahead and go first since you were the first...

(Jonathan): This is (Jonathan). None for me.

John McElwaine: Thanks a lot. This is John McElwaine. The question I have, it's not a easy one to ask and have answered on this call but perhaps we can do it is I gather from what I heard that there may not be a lot of interest in the participants on this call in being a validation provider.

And I want to make sure that I am getting the right understanding from the call. And so I would just sort of generally ask whether any of the participants would be willing to be a validation provider?

In other words, would you be willing to accept a set of standards and then enforce those standards through a certification process?

Ken Michaels: It's Ken Michaels here. I think as an accounting firm -- and Tim correct me when I say this -- but as an accounting firm we're already bound by certain restrictions as it were when providing attestation type certification. So we're bound by the AICPA or the local or more country-based accounting guidance.

So I don't think that would put us in a position to be bound by any other broader guidance meaning we wouldn't be in a position that we would be a certifier in running the program.

What we could do what we do for other attestations is be one of the people that goes and evaluates companies.

So while we couldn't be administering the program we certainly could participate if the criteria aligns with our AICPA criteria basically.

((Crosstalk))

Kathryn Holt: To add to that for - Kate from Ernst & Young. I think the one key here is that as we look at some of the things that we do and the way that we attest, it's based on objective and measurable criteria.

And I think that if we got to the point that we were executing against objective and measurable criteria we would be able to provide a level of attestation.

But, you know, again, the way that we're bound couldn't necessarily manage a field program.

Tim Davis: Yes this is Tim from Deloitte. I would agree with Ken and Kate. The AICPA rules require there to be what are called suitable criteria. And Kate, you know, mentioned probably the most important of those.

But suitability really speaks to other criteria defined in such a way that someone looking at this and looking at the opinion we've issued might get confused. And I'll give you an example.

The criteria are worded in such a way that there's a certain aspect of security that gets left out that a reasonable person would expect to be included.

They see our opinion and they assume that, you know, all is good and that it would include that reasonable concept. So I guess the answer in terms of whether we prepare to participate really depends I think on both the criteria that we eventually end up coming up with and then also how the program's going to get structured.

Because I'll tell you to be candid, I mean many of the CPA firms are not in the PCI validation space because of the way their program ended up getting structured.

And it comes down to certain aspects are not consistent with the CPA guidelines. And also they were structured in such a way that really creates an unacceptable risk for the CPA firms.

And so I think those are the two principle considerations is one is it suitable with our attestation rules that we'd have to comply with?

And secondly, is the program going to be structured in such a way such that we can suitable mitigate the risk as auditing firms that we would be taking on?

Man: Yes, just for the Advisory Board, just a quick overview of how we function. So basically we're bound by these AICPA standards.

We've got these attestation rules that let us do certain things. If the things we measure, the criteria Tim referred to, comply with objectives and measurable et cetera, et cetera. So as long as your criteria that you put as far as this program fits into that, then we leverage the AICPA attestation standard to deliver an opinion level service.

So we won't look for any other ICANN. And that covers us under independence. It covers everything, that attestation standard. So that's what I think it sounds like most of us want to leverage on this call.

Then it comes down to them just defining the criteria so it fits into that in such a way that it allow us to deliver this much like a (SYS) trust, a SAS 70 -- that type of concept.

Mark Lundin: This is Mark with KPMG. We'd certainly be interested in, you know, participating in that as well. And I saw in the responses to the questions that, you know, the group was certainly willing to, you know, to deal with feedback and any fine tuning of the criteria to make sure that they were auditable within the auditing standards.

John McElwaine: This is John McElwaine and I'll ask one more sort of follow-up question to that which is if it falls within the IACPA standards is there any just general prohibition then of there being a seal program relating to having me those criteria?

Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

Tim Davis: This is Tim from Deloitte. That's a complicated issue is the seal program because one of the things the AICPA regulates is basically the form of the reporting that the auditors are allowed to produce.

Now the AICPA and in Canada the CICA do run their own seal programs and have got certain sets of criteria for different types of situations. On is called WebTrust, another one is called SysTrust.

The terminology around those are actually changing to SOC 1 service organization control. One - SOC 1, 2 and 3 for the three different versions next year.

So that would be one consideration. If you're wedded to a seal program would be engaging with the AICPA and the CICA to accommodate this through one of their existing seal programs.

And that would then automatically fall within all the auditing standards. But if - so and here's the distinction.

If ICANN wanted its own seal then I think what you would have to do is you could engage an auditor to come in and issue an out of station report. They would issue their findings to some ICANN body to say here's what we found.

And that could be either an examination level opinion that results in an opinion being issued or it could be what are termed as agreed upon procedures. Where certain procedures and the results of those procedures are reported back.

And then it would be ICANN that makes the final decision. And then in that instance it's ICANN seal that's going up, not the seal that's sort of endorsed by the auditing firm.

Mark Lundin: Thanks. That's very clear.

Craig Schwartz: Got any follow-up before we move on?

Mark Lundin: I'm good.

Craig Schwartz: Okay. Mikey?

Mikey O'Connor: Thanks. This is Mikey. Building a little bit on this part of the conversation one of the questions that I've had throughout this and would be very interested -- not on this call per se but in your responses in hearing about is whether you think this will work.

The list of criteria is very long and very detailed. It's sometimes familiar and sometimes new.

But in this request for information cycle one of the things that I as a member of the committee would be really interested in hearing is just your candid assessment as to whether this approach will actually make these domains more secure or not. And I would like to highlight that the committee is not at consensus on what to do.

And so your responses are likely have a substantial impact on the final outcome here. We've got a bunch of pretty fundamental issues that we have not resolved in the committee.

And sometimes the documents are more forceful than the underlying opinions that created them. So not so much a question as just a request for all of you when you're filling out your responses and take and aside and say thank you very, very much for all of you who are going to do that.

Please in addition to sort of taking the technical view which is what we've been discussing a lot today also give us your thoughts at sort of the strategic level as to whether what we're trying to do here is actually going to accomplish our objective which is to make the TLDs more secure. Thanks.

Man: Hey Mikey just a quick follow-up to that. Have you had registries or registrars interested in the program in becoming certified?

Like is there a demand that's been driven at any level?

Mikey O'Connor: I hate to speak for whole groups like that. But there are several - there's at least one or two registry and registrar members of the committee.

They are not on the call today and aren't part of this sort of stalwart hang in there gang. A couple of them have expressed pretty strong reservations about this program.

One of them asked a rhetorical question one time on a call saying aren't we running the risk of creating a really expensive ghost town. And so I think there is a question there.

There certainly isn't a group of registries or registrars just beating down the door asking for this. This is really coming from a different place.

Note: The following is an unofficial transcription of the meeting. In some cases it may be incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the session, but should not be treated as an authoritative record.

But, you know, I'm also just a member so I'll leave it to the fearless chair to maybe flush that out a little bit.

Lynn Goodendorf: Well I'm not the chair but this is Lynn Goodendorf. And as a member of the advisory group I thought I would actually kind of bring up the point that our advisory group has tried to envision the future of more TLDs.

And so Steve's question about how this fits with the guidebook for the new TLDs I think is very relevant because I believe that that's what generated or prompted ICANN to have this - have a look at this is -- I don't know that anyone knows the answer but we're trying to imagine what it would be like with many more new TLDs. And would there be a demand for some of those TLDs to want to differentiate themselves in some way by offering some type of assurance or distinction that they are making extra efforts on security.

And in our group we've talked a lot about how we cannot guarantee -- no one can guarantee absolute security. It's all relative.

And so the idea would be would a TLD owner want to differentiate themselves in that way. And if they did want to differentiate themselves in that way how would they go about doing it.

So I just thought I would add that. And again I would like to thank all the people who've responded, you know, so far on the RFI.

And your input has been valuable. I think this call has been very helpful to me.

Thanks. That's all I have.

Paul Smocer: And this is Paul again. You know, to answer that question from my perspective a bit, you know, I think I would see that the HSTLD program grew out of probably a couple stimuli.

One was the work that was being done around question of limiting malicious conduct on the Internet which partially drove this. Part of the stimuli was that speaking for my industry which is financial services we are very interested in assuring that any new TLDs that are primarily offering financial services are as secure as possible.

So I think, you know, the question of demand, those that would be coming from the financial services sector probably are driving some of the effort here. And would be ones that would be interested in some sort of validation of their security but are more fundamentally interested in very secure TLDs being created.

So just in close...

Man: But that doesn't affect the registrants who have demand. They're not registries or registrars.

Paul Smocer: Well, you know, I think if - we'd obviously be looking at the spectrum of entities involved. So, you know, you're not going to have good security in a TLD if you don't have some of the effort coming from the registry.

You obviously probably, you know, and I don't want to reopen the debate here with the group. But - and this was the question that was asked earlier about registrar versus registry.

There are obviously some things the registrar needs to do to help assure security and resiliency as well. But, you know, it is - there are multiple parties involved and each of them plays some role in the secure chain if you would.

And that's again my opinion given my perspective on what industry I'm in. So - but I think, you know, in terms of demand at least from our industry's perspective and we're working with multiple parties in the industry, I think you would see some demand in that space.

You know, there is unfortunately a lot of malicious conduct that is focused on financial services. There is a lot of fraud that results from bad conduct.

And fundamentally we're trying to protect our customers in that space as much as possible. So that's certainly a driver for us.

Let me go back to -- Lynn is - are those the only comments you wanted to make? Did you have any questions?

Michael Palage: Yeah I think we're probably done all of the - this is Mike Palage. I think we've gotten everybody.

Craig is there anyone else, any other committee member who has not yet spoken? I think you - (Jonathan) are you on? Do you have any comments?

Okay, sounds like...

Man: Mike, (Jonathan) indicated initially he did not. So...

Michael Palage: Okay.

(Jonathan): I do not Mike. Sorry I was clearly muted, yeah.

Michael Palage: Okay. So what I'd like to do here and as I said perhaps the potential respondents could see some of the rich discussions that had - that the group has been engaged in over the last year.

What I'd like to do is before wrapping up this call is perhaps if we could just go through based upon some of this dialogue between the advisory group members are there any sort of follow-up questions or comments that you might have?

And if not perhaps I could just turn it back to Craig before wrapping up the call. So Paul do you just want to go through and just see if there are any comments?

And then we perhaps begin the wrap up?

Paul Smocer: Sure. I think you just made the offer Mike. So I'll just extend the offer again.

If there are any follow-up questions or comments, you know, I think from an - and Mike or any of the group correct me if I'm wrong on this. But I think from a next steps perspective we're going to digest the information we heard on this call -- all of which was very good.

And let me add my personal thanks as well not only for the original interest and the original questions but also I thought we had a lot of great information from the participants on the call today which I think will help as we form our final look at this program.

And so I really do appreciate that. But again any follow-up from anything that you all heard that you would like us to take away?

Steve DelBianco: This is Steve DelBianco. I would certainly ask what you plan as the next step.

And that'll help us to focus the kinds of questions that would inform the next step of the advisory group and staff.

Michael Palage: So the next step - let me step in here as chair. The next step Steve is we will probably have a - our next - we will probably have a call next week in which we will digest...

Man: Did we just lose Michael?

Steve DelBianco: Sure sounds like it.

Man: He's probably saying something brilliant too.

Steve DelBianco: Yeah it's probably really good. Dang it.

Paul Smocer: I'll just follow-up with that. I think where he was going was that, you know, I think it'll take us - in our next call we'll certainly go over what we heard today and digest what we heard.

And I think one of the things that's probably - and figure out is between what we heard today, the work that we're continuing to do with ICANN around the question of, you know, its involvement particularly in the validation process. I think our next step would be to try and figure out essentially what that validation process would involve.

And how we might structure it given ICANN's support, given what we heard today particularly with regard to who might be able to manage a program like that for us if ICANN is not kind of taking management oversight for it. I think it was very revealing to hear that stuff about the AICPA requirements in particular.

And that essentially precluding one of you folks from necessarily managing the program as opposed to serving as validators or certifiers. So I think we need to digest that, come up with what our next step will be to take the program forward in terms of the validation process based on what we heard today.

And then I would imagine we will loop back to you with kind of an update on where that stands and how that might take your continuing involvement to execute on it.

Craig Schwartz: Thanks Paul. This is Craig and I just got a message from Michael Palage that he did get cut off.

And he said it sounded like we're on the tail end of the call anyway and that you've done a really good job in wrapping this up. In terms of schedule going forward as Paul just said -- and I think Michael did before he got cut off -- we'll probably have a call next week to digest what we heard on this week's call.

And then the intent is to look forward to everyone's responses for those that will provide a written response by the 17th of December. And then reconvene a weekly advisory group call starting I believe on Wednesday, January 5 leading up to the publication - I keep calling it a final report but maybe that's not an accurate term.

Maybe it's just the summary of the report of the findings from the RFI process that we would anticipate publishing sometime in mid to late February in advance of ICANN's Silicon Valley public meeting scheduled for early March. So it's kind of a very high level view of next steps with regard to the schedule.

I would just suggest to any folks that are on the call -- particularly the folks that posed the questions -- if there is follow-up that you have from this call that we need to engage with you on, obviously we can do that by e-mail. And we can also set up another call if need be.

But otherwise we hope to hear from you all by the 17th of December. And to gain enough information that this group can proceed with a report and some recommendations to ICANN on how they think the organization should proceed with such a program.

And unless there are any further questions or closing remarks from any one of the advisory group members or for that matter from the folks that are posed questions, I would suggest that we're probably in a good position to wrap up the call. I thank everyone for your time and the questions and the commitment to helping move this process forward.

And I will open the floor back up for a moment and then we'll wrap up.

Steve DelBianco: Craig it's Steve DelBianco.

Man: Hi Steve.

Steve DelBianco: The questions, can I get in a few on that.

Craig Schwartz: Sure.

Steve DelBianco: Mike opened the call by listing off what he felt was the consensus items that have been reached. And I wrote two of them down.

And want to ask the other members of the group if there are other potential items. Just posted down that Mike said there was consensus to enhance security of TLDs including existing and there was consensus the control elements had to go all the way down the value chains.

Was there anything else that you guys would say the group has a firm consensus on at this point? Like as to whether or not it'd be mandatory? As - when it ought to kick in and whether it should affect the guidebook?

Any other consensus items we should all know about?

Mikey O'Connor: Steve this is Mikey. Just to correct one thing -- I don't think we have consensus that it goes all the way down the value chain at this point.

Steve DelBianco: And - thanks Mikey. Are there any other items about which you do have consensus which we - which I didn't list?

Lynn Goodendorf: I believe that - this is Lynn. I believe that we did have consensus that it would be a voluntary program rather than mandatory.

Steve DelBianco: Thank you.

Paul Smocer: Yeah I would agree with that too Lynn. This is Paul.

I think at this point we are envisioning it as a voluntary program. I don't know that we have specific consensus on it.

But I would say our lean at this point is that at the moment at least it looks like it would apply only to new gTLDs and not existing. Though they could certainly partake in the program.

But our focus has been around the new gTLDs and not necessarily existing gTLDs.

Steve DelBianco: Thank you.

Craig Schwartz: Did you have a follow-up to that Steve or...

Steve DelBianco: Just - that's all great. Thank you.

Craig Schwartz: Sure. Anyone else either from the advisory group's side or from the participant side?

Tim Davis: Yes Craig - sorry Craig. This is Tim from Deloitte.

Just one of the final comments - I'm just going back to some of the comments. I believe it was Paul made earlier about our financial institutions that may be looking to use new TLDs for the provision of financial services.

It kind of got me thinking a little bit about just a caution about I think you do need some consensus on the scope of what you're defining as security. Because to the extent you're getting into security over the customer's financial data and let's say, you know, other things like that that may be higher level issues as opposed to say the operations of the registry you are going to not only, you know, add significant more complexity to this.

You're also going to start to overlap with existing financial services regulations that they have in that regard. And at least, you know, from a financial institution's perspective they're going to want to have as much consistency as possible with what it is that they're complying with.

And so, you know, if you want to go to that space you would want to make the expectation as consistent as possible with the existing rules that are in that space that govern financial institutions and not create something different. Because that's probably the biggest - one of the biggest hassles that financial institutions and all businesses in generally have quite frankly when it comes to new regulations or new standards is the fact that they conflict and don't align well with one another.

And...

Paul Smocer: Let me just jump in if I could. I mean, you know, as I did mention probably for my perspective on the stimuli was the industry that I'm in. But on a personal level versus representing that "industry" I do find it a little difficult to believe that we would be the only industry that should be interested in that kind of level of security around TLDs.

I would like to believe that whatever TLD might be created that is servicing the healthcare industry would be interested in, gee because I'd sure like to know my healthcare information was protected. So, you know, I didn't want to infer that while we're interested that suggests that we would be the only industry that would be interested.

And therefore whatever we come up with should align with the requirements of the financial services industry only. You know, I think being a part of this advisory group while I have a motivation to make the world more secure for financial services I have a broader motivation to make it more secure period.

Lynn Goodendorf: This is Lynn Goodendorf. I agree with that Paul.

Also as our advisory group did an initial draft on control objectives we did have quite a bit of discussion on this that it was our desire and intention to not duplicate other security standards such as PCI or any other regulatory type requirements.

Our thinking was to try and develop a criteria and security objectives that would be tailored to actually the domain name world. And for this particular type of service.

And - but we did have quite a bit of discussion on it. And we also as an advisory group I believe had a consensus that we were not going to try and be detailed.

But that we were going to focus more on what I personally would call control objectives -- giving people the latitude to decide how to implement or how to design ways to achieve those objectives. So that's just a little bit of my perspective from the advisory group.

Craig Schwartz: Any further questions, comments or remarks from the advisory group or from the participants? Well hearing none I'd like to once again thank everyone for participating in today's call.

To commit to making ourselves available -- that is the advisory group -- for follow-up questions or clarifications that need to be made so you have the information you need to respond to the RFI. I think everyone has my contact information and I can certainly route anything that you might have that you would like distributed to the advisory group.

I'm happy to do that for you. As I said at the onset of the call an MP3 recording of this will be posted to the HSTLD information webpage on the ICANN website.

So everyone is free to have another listen at the dialogue. And I think with that we'll wrap up and say thank you one final time.

Man: Thanks all.

Man: All right.

Craig Schwartz: Thanks everyone.

Man: Thank you Craig.

Woman: Thanks.

Man: Thanks bye.