Inter-Registrar Transfer Policy Part B PDP
Transcription
Tuesday 01 September 2009 at 14:00 UTC

Note: The following is the output of transcribing from an audio recording of the Inter-Registrar Transfer Policy Part B PDP call on Tuesday 01 September 2009 at 1400 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://audio.icann.org/gnso/gnso-irtp-b-20090901.mp3
On page:
http://gnso.icann.org/calendar/index.html#sep
(transcripts and recordings are found on the calendar page)

Participants on the Call:
Michele Neylon - RC
Kevin Erdman - IPC
Miriam Trudell - IPC
Barbara Steele - RY
James Bladel - RC
Berry Cobb - CBUC
Anil George - IPC
Paul Diaz - RC
Tim Ruiz - RC
Eric Brown - RY
Michael Collins - Individual
Mick O'Connor - CBUC
Graham Chynoweth – RC
Rudi Vansnick – ALAC

Staff:
Olof Nordling
Marika Konings
Glen de Saint Gery
Dave Piscitello
William McKelligott
Gisella Gruber-White

Coordinator: The recording has started madam. Please go ahead.

Gisella Gruber-White Lovely, thank you. Good morning, good afternoon to everyone. I'm going to do a quick roll call. On today's call we have Michele Neylon, Barbara Steele, James Bladel, MiriamTrudell, Kevin

Erdman, Mike O'Conner and Anil George, Paul Diaz, Tim Ruiz, Michael Collins. And from Staff we have Marika Konings, Glen de Saint Gery, Olof Nordling, Dave Piscitello, William McKelligott

And if I could just remind everyone to please state their names when they speak for the accuracy of the transcript. Thank you very much.

Michele Neylon: Okay. Did you all get a chance to have a look at the agenda for this afternoon's call? So, okay. (Dave Pasticalo) has taken some time out. And I believe (Dave) is going to go over some of the (S-Sacs) and findings. And then after (Dave) has done that then we'll move on to some of the other points on the agenda.

And (Dave) would you like to kick off there please?

Dave Piscitello: Okay. Are you speaking (unintelligible) from the 2005 (unintelligible) report or are you more interesting in the relationship of the more recent report that (S-Sacs) published on (detective) measures?

Michele Neylon: I think the thing is that some people on this call would be very familiar with issues going to as far as 2005 and beyond, where as some other people are kind of new to some of the topics here. So in some respects I think you need to kind of work on the basis that we might learn quickly but done presume that people know everything from the get go. If that makes any sense.

(Dave) can you hear me?

Marika Konings: (Dave) we can't hear you. He's still listed as connected but.

Dave Piscitello: okay. So it's not just me?

Mike O'Conner: No I can't hear him either. This is (Mikey).

Michele Neylon Okay. While (Dave) deals with his technical difficulties let's move on then. I suppose. (Dave) if you can hear us. (Rikka) can you call (Dave) or something?

Marika Konings: Yes, I'm jabbering him, so.

Woman: (unintelligible) has an issue but I think he hasn’t figured out how to solve it. I mean to kick it off, I can maybe briefly take people through the two slides that are up here introducing the issue.

Michele Neylon: Okay.

Woman: Are do you prefer to go to some of the other items on the agenda?

Michele Neylon: Does anybody have a preference? I honestly don’t mind one way or the other.

Mike O'Conner: Hello, this is (Mikey). I'd say let's carry on and see if (Dave) can rejoin.

Michele Neylon: So we look at the slides that we have up there and let Marika go through those first?

Mike O'Conner: Yes.

Marika Konings: And (Dave is trying to dial back in. So just very briefly Issue A looks at rather an expedited handling process should be developed for a fraud situation. So the report highlights there are a number of suggestions that were made is the Staff Report in 2005 after this issue was raised in a public common period.

And there are a number of issues were considered or raised as possible (unintelligible) in developing an expedited handling process and looking at automatically returning names that are subject to a dispute has been resolved or automatically rolling back the name servers.

And the (unintelligible) produced a high (decking) report and I'll wait for (Dave) to return to talk a bit more about that. In which (Dave) provided some more details about how such a process could look like and they highlighted some elements as an emergency action channels, a companion policy to this emergency action channel and a public awareness campaign that could go with that some that people are aware that it’s a way they could address problems in this area.

(unintelligible) some of the question that we identified in Asia's report that might need further consideration is like what is the extent of this problem? Does it actually warrant the development of a separate policy? Or is it currently better served by interaction between registrars that might be able to handle these kinds of situations in a quicker way?

Is it maybe better to have best practices in stead of a policy? How do you ensure a fair process? How do you avoid that people might evoke this procedure just to stall return of a domain name or to hold onto a domain name that’s not theirs?

Who would be in the end a decision maker? Whether a domain name is actually been hijacked or was it a proper transfer? And are any market solutions or best practices that already exist that might address this issue?

(Dave) are you already back on the call?

Dave Piscitello: Yes I'm back on the call. I'm sorry. I was using voice over IP and my provider is having some problems today. There's some very bad latencies. So I switch to a land line I hope that solves the problem.

Do you want me to, I guess I should probably start from the beginning. I have no idea what you heard and did not hear.

Marika Konings: Yes probably. What I just did, I just quickly went over the slides that are up and just talked a little bit about the recommendation to Staff Report and some of the questions that the group might want to consider in relation to this question. And I just briefly mentioned the (S-Sac) Report but I didn’t go into any details of the recommendations you made there so I'll hand it back to you on that one.

Dave Piscitello: Okay. Again apologies for the disconnect. So there are actually two relevant data points and reference points with respect to (S-Sac) interest in domain transfers and both focus primarily on unauthorized transfers resulting from some form of hijacking or some form of unauthorized access to a domain registration account.

In 2005 we actually wrote a report called Domain Name Hijacking, (unintelligible) Directs, Risks and Remedial Actions. And in that report what we've focused on were some high profile incidence were a domain account was accessed without authorization and either the domain was modified in such a way were the DNS configuration pointed an otherwise legitimate user to an impersonation site or to a defacement site.

And from some of those incidences one of the things that we observed was that some of the victimized registrants experienced what they considered very, very long delays in actually getting their name back. Very much like a fishing attack, one of the sort of metrics that people consider in terms of restoring service when business is interrupted is something measured in minutes and hours, not measured in days.

And so one of the goals of (S-Sac) had without pointing fingers at anyone, was that it would be useful if there were some guidelines that would allow registrars to acknowledge that there had been a malicious act and restore domain and restore what we call the last working configuration so that the victimized party could restore his business service and continue his business following the interruption without a problem.

We felt that that would was addressed adequately in the existing policy and contract so we encouraged the community to study this issue. I don’t there's very much point into going into very much more detail then that from the 2005 report.

Essentially our focus was primarily on what we consider a similar activity to a form of accelerated suspension in the case of a well documented and identified domain use for fishing or illegal pharmaceuticals or some other malicious act.

Just recently we published a report called (Sacs) Number 40. And it's called Measures to Protect Registrants from Malicious Use or Exploitation of their Domain Registration Accounts. And in that document we actually focused less on the transfer policy and more on measures that registrars could consider and encourage registrants to employ as well that would prevent or at least seriously reduce the opportunity for an attacker to compromise a domain name account.

And either do some sort of malicious alteration of DNS or change a contact for a subsequent attempt at a registrar transfer, registration transfer rather. I'm not certain how much more you want to know about what we've done. IN (Sac) 40 we talk about things like stronger registration verification processes, the use of perhaps multiple party confirmations before one would accept a DNS configuration or a multi party confirmation before one would allow a transfer to progress.

And so the model here is very similar to the kind of 1950s movie where you have or even Golden Eye if you remember the James Bond movie where you have to have two people with complimentary keys before you actually can launch a missile and in this particular case it would be two people who would have to in some way proactively respond and confirm before a registrar would begin or accept a transfer of a domain.

There are some other measures that talk about things like multi (factor) authentication, having the registrar either through an (unintelligible) or some other kind of method provide assurance that the registrant identifies a unique party for administrative contact, a unique party for registrants, a unique party for technical administrator.

We also talk about using methods other then electronic mail and making them available perhaps as an option or an additional service for a registrant so that the registrant could say in the event that I do get hijacked it is very possible that the attacker might modify my mail records in my DNS and then I wont get electronic mail. So one of the things that I might want to do is take note that I want the registrar to contact me using some non email method, either an instant message or a phone call or some other method.

So the report is fairly detailed in providing a very long item list of possible measures that have been used in other vertical markets like the financial markets, sort of like secure enterprise intranets to provide stronger measures at the gate sort of speak to seriously reduce the opportunity for intrusions that lead to hijacking.

And much less emphasis is placed on looking at the transfer element other then the fact that that is one of the activities that we would (swort) if we had stronger verification measures and stronger confirmation metrics and measures.

Man: Okay, thank you. Does anybody have any questions?

Kevin Erdman: Yes, this is Kevin Erdman. One thing that struck me as I was looking at the report and listening to your description is whether there are, in addition to the technical means to try to protect things and (add) security and verification and all of that, are there technical ways that one might be able to determine a difference between a valid transfer and a hijacking type of case? You know for instance different traffic patterns or, you know causing some erratic behavior in terms of what the use of the web site was originally prior to the transfer and after the transfer?

Dave Piscitello:I don’t know of any study that has been done in that area of (anotally) detection. And if you think of the (cause) protection, I think of the broad scope of the way domain manes are used from (pasting) all the way to someone who has had a domain since the (jompus cell) writing on a napkin era. I think you could come up with a set of potential markers that’s used in combination would give maybe a fingerprint of some sort of malicious activity.

I think that they would be very hard to formulate. My guess is that a better or I speculate that perhaps a more fruitful way to invest some research would be to go to some of the people who would be most concerned about the transfer of what they believe is a asset like EBay or Pay Pal or Amazon and ask them what specific measures they might consider.

And that’s one of the things that (unintelligible) in this report and I think preventative measures are complimentary to what you are attempting to do with improving the transfer process. As we reduce the opportunity to break in, we also reduce the opportunity to actually do some sort of malicious act.

One of the things that you could look at is the quality of the registration contact information and as an example if I'm transferring a domain that has been held by a party for many, many years and the domain registration data is complete and to the best of the registrars ability to (daduse) accurate and then it's being transferred to a party where they haven’t provided what looks like or what is interpreted as a correct phone number or the address is not complete and the email address doesn't actually, you can check to see if the email address is active and its not or its in a Gmail or a Hotmail or some other or a spam domain like 123, xyz, 456, 2.cm.

You could probably start to put together that sort of analysis but I don't know of anyone who's actually done something like that yet. Perhaps one of the larger registrars might be looking into that in their use research. But nothing that I know has been surfaced yet.

Michele Neylon: Anybody else have any other questions or comments? ((Mikey)) and (Tim). Okay, we'll take ((Mikey)) first then.

Mike O'Conner: This is (Mikey) O'Conner. (Dave) just to clarify is it safe to say then that the (S-Sac) is sort of leaning away from the 2005 emergency action channel recommendation and leaning more towards stronger security multi factor identification etcetera?

Dave Piscitello:I think they're complimentary Mike O'Conner. Security is always about multiple lines of defense and multiple lines of detection so you do as much as you can to keep intruders out. But once the intruders is in you don't want to just let him have free access.

And if he manages to steal something and a hijacking isn't in some context a theft, you want to be able to provide the victim with some recourse. And so I wouldn't characterize (S-Sac) as saying if you do everything up front, you don't have to worry about anything in the back.

Because no matter how good the defenses are, there's always the possibility of social engineering, or coercion or some other manipulation of a domain registration account that could result in an authorized party doing something with the domain he how has control over. So I think that, and I think that in a very simply business case like the one with (Panics) or with icann.org the domain is misused in a much more complicated case the domain is put in a limbo state and perhaps its not just an attacker but its some sort of situation where a customer of an ISP has registered a domain.

The ISP decides the domain has some sort of value and he's not particularly decent guy and he's registered it on behalf of the customer. And now you have an issue were you have to work a little bit harder but in the mean time the there's just been an argument over the phone and the (ISC) is a small guy and he just goes and he changes the domain and moves it to parked or to whatever else he wants. You know, the guy who's running (Alice's) Banana Factory is not selling bananas.

And I think there is an appropriate course other than lots of money and lots of time elapsed.

Mike O'Conner: If I could ask one follow up question from (Dave). Looking at Marika's slide, there are sort of four pretty tasty questions, the extent of the problem, how to ensure a fair process (unintelligible) the decision maker and which market solutions are best practices already exist.

Does (S-Sac) have any opinion about those questions at this point that we don’t already have available in the form of the reports?

Dave Piscitello: I would honestly say that (S-Sac) has not looked at these questions. I think that there are some models that are emerging in the area of accelerated suspension processes that have come out of some work between registrars and the APWG that might be applicable here.

I think, my personal view and this is not a (S-Sac) view or an ICANN view, is that there is room in the domain name world for an accredited intervener. And it’s a trusted party that either through bonding or through certification or some other mechanism registrars can all have relatively high confidence is going to present them with legitimate as opposed to (specious) cases.

And if we could agree on such a model where there are people we trust who are going to go and do the work and much in the way that we trust attorneys and accountants to provide us with accurate information. Then I think that those are the kinds of people that we should recognize and use to provide some of the aspects of the fair process.

So if I had someone I could go to much in the way that many of the brand owners use, companies like (Internet Identity) or some of the registrars who provide online brand protection go and say I want you to help me if somebody starts to infringe on my brand, let me know, bring me the appropriate information. I'll go to the registrar with your information because I have high confidence your not going to come and tell me that this domain is fishing when its not.

And I think those are valuable. And people who do those have very high reputations marks, so I think we need to study those and come up with one for the industry so that registrars have a relatively high confidence that, and I think we can compliment that with some sort of safe harbor mechanisms that allow registrars to take an action without an enormous amount of liability and risk of a false-positive.

Mike O'Conner: This is (Mikey). I'm done. Thanks (Dave) I'm really glad I asked those questions, that was terrific.

Man: Michael Collins had a question I think.

Michael Collins: Yes, but (Tim) is ahead of me I think.

Man: Well I'll do the two M's first and then we can go to the T.

Michael Collins: Okay. Very good. My first question I'll wait to ask a follow up possibly and it's really of the group as much as of (Dave). Are we within our charter to be dealing with registrant changes? Obviously it's not the same as a registrar transfer for the registrant to be changed or the name service to be changed. And its not that I don’t think these things are important to and shouldn’t be dealt with, but I just wonder if that’s including in where we should be. Or is this a security issue that’s outside of inter-registrar transfer issues?

And the second is just well I'll let the group answer that.

Tim Ruiz: This is (Tim), I'll comment on that is it's okay?

Man: Please (Tim).

Tim Ruiz: I think its okay to look at that. When you look at the different (unintelligible) of what's in our charter and the questions being asked, I mean in reality they all have an effect on the registrant and I think that many cases that’s really what our primary concern is, is you know making this process safe and secure and understandable and easy to use as possible by the registrant.

But I think those are valid questions to ask and whether we're able to, that might affect the ability to actually have a policy to some extent I think because we have to take into account various registrants needs and that types of things.

But I think those are valid questions to ask, you know what is the effect on the registrant? Or how do we make things, how do we educate the registrant? And those types of questions, I think are important.

Mike O'Conner: This is (Mikey), I'd like to comment on Michael's question too. I think that to a certain extent one of the reasons that this relevant to the inter-registrar transfer group is because a hijacking which immediately moves the domain to a different registrar is a different sort of event then one that the domain stays within the same registrar.

I think when it's in the same registrar it's probably a bit less complicated to deal with. And because we are interested in cross registrar transfers that this relevant.

Michele Neylon: Personally I'd agree with that as well this is Michele speaking. If the changes of what it appears as the registrant and it will obviously have an impact. I mean one possible situation is where the registrant details may need to be undated because they are no longer valid and it could be that an employee has moved on or it could be any number of different reasons.

But I still think its pertinent and it relevant. And going back to people with their hands up, Michael I think if you could put your hand down please. (Tim Louis), you wanted to jump in there?

Tim Ruiz: Thanks Michele. Yes, two, not so much questions, I guess as just two concerns I wanted to point out that I feel we need to keep in mind. One (Dave) sort of touched on and that this safe harbor concept. I think that’s going to be important to registrars when we're talking about providing an entity or a process that they can rely on in order to take action on quickly.

That a lot of, you know the time that it takes and the concerns the registrars have with doing things much faster, you know a lot of that centers around just doing do diligence to make sure that they're doing the right thing.

And protecting themselves from potential legal (risks) later. And those shouldn’t be under estimated, they can be huge especially when we're talking about the high profile sites or sites that, you know there's a high amount of traffic and reliance on, we do the wrong thing and there's a huge potential risk involved with that.

So, that needs to be kept in mind as we move forward with any kind of recommendations.

Michele Neylon: (unintelligible) (Tim) please. What's the safe harbor concept you're talking about?

Tim Ruiz: Well in other words some sort of protection from a registrar who takes action so that they're not later, it minimizes to the extent possible the risk that they'll end up in court with some, you know spending millions of dollars trying to defend themselves over having taken action. That what I'm really referring to.

So for example what Go Daddy will do in some cases when we need to transfer a name back and we, you know working something out directly with the registrar involved is (indemnifying) one way or the other the other registrar in order to make that happen without having to go through the dispute process which would take much longer.

So registrars are kind of doing that between themselves, some are more inclined to do that then others. But so that’s not a perfect solution but it's just an example of one of the things that's going on.

The other issue that I want to point out is just the volume that some registrars have to deal with and there's probably a flexibility (unintelligible) perhaps more then anybody else but I can't imagine it doesn’t affect registrars like (unintelligible) and other network solutions.

But just giving an example when it comes to transfers in and transfers out, we deal with one of those every 30 seconds on average. So that’s the volume that we're talking about. So things like calling people on the phones to verify this or that gets to be, you know a bit problematic, we'd practically have to double our staff just to deal with something like that.

Especially when that’s just transfers. And then we'll do, we register new domain names like every one or two seconds but that doesn’t even include the millions of transactions that take place that involve, you know changing name servers, contact details, etcetera, etcetera.

So the volume can get quite high and that’s not just Go Daddy, I think you'll find that with other registrars as well even though there may be somewhat less volume, it still stacks up when you talk about the number of transactions involved. So that needs to be kept in mind too as we think about possible solutions or recommendation that might solve some of these problems.

Mike O'Conner: (Tim), this is (Mikey). I have a follow up for you. Do you have a sense of the frequency with which contested inter-registrar transfers happen? You know at first I thought you meant one of those every 30 seconds and then I realized that you didn’t mean that.

Tim Ruiz: No that’s probably some information we can get. I think we were trying to gather some data on that. I'm not going to speak to it. I think (James) has been working on that. I'm not sure he's prepared too either yet today. But I think the (unintelligible) important because if when we're talking about measures that might preempt the possibility of a problem occurring. So I think there's two issues, one is okay something's happens, now let's get to a quick resolution.

And that’s where (unintelligible) issues need to be dealt with and then other things we've talked about that (David) talked about too, dealt with things that can be done up front to prevent a problem form happening. And that’s where we have to think about the volume of transactions that are occurring at British registrars.

Dave Piscitello: And I agree. This is Dave again. One of the things I want to be certain people understand about the (SSAC) document number 40 is that these are measures that we suggest registrars consider for customers who are seeking better protection.

There might be at some future point in time an (S-Sac) document that says, you know the overall security baseline could be improved by doing X. Where X might be a different list but right now we're saying that there are companies that either through lack of understanding or lack of available services might benefit from having additional measures.

But certainly automation and dealing with transactions in high volume that are atomic events that occur in virtually seconds has to be a factor in a service that scales to serving millions of users with millions of transactions per day or week or even moths.

Michele Neylon: Okay. (James) you had your hand up. Do you want to jump back in?

James Bladel: Thanks and I think (Tim) and (Mikey) covered a lot of my questions. So I'll go ahead and lower my hand at this point. I did have a new question that just kind of popped in my head there for (Dave) relative to the (S-Sac) report in 2005 and (S-Sac) 40. And this question (unintelligible) by extension goes out to (Barbara) and (Erik) and any of the other registry reps on the call.

What is the role of the registry in transfer security in general? How do they view themselves as just interested observer or taking what the registrars give them on face value? Or is there some sort of a at least a detection and notification that there's anything a miss with the transfer patterns?

And I'm curious is if this is a solely a registrar focus issue or if there is some role for registries as well?

Barbara Steele: This is Barbara, I'll jump in here. From our perspective I would consider us more of an innocent by stander if you will, to the extend that a registrar submits a transfer request to the registry and provides the (authen) code to validate that. And again, this is strictly registrar to registrar transfers because here at (VeriSign) obviously we don’t see any registrant information so we have no visibility into that.

And then basically if there is an issue that arises, you know we do get involved if somebody submits a transfer dispute case relating to a registrar to registrar transfer. So I would almost view this more as an issue that is, I'm not going to say its exclusive to registrars but I would say that it is primarily impacting to registrars.

Obviously the registrars also form the relationship with the registrant at the registry. We obviously can look at rolling out new products. It may help to secure at least verifying made server changes, things like that, that we can work in conjunction with registrars on.

But beyond that strictly registrars to registrars transfers is all we really see as long as there is a (authen) code we trust that the registrars that’s surveying the transfer has done the do diligence on their end to make certain that it’s a valid transfer.

James Bladel: Thanks Barbara. This is (James) again. I kind of suspected that was the case. But I wasn’t sure if that, if you guys feel the same about any sort of hypothetical (urgent) return process and whether the registries would also play a role in that.

Dave Piscitello: I do have a question because one of the things I'm curious about is the extremely high profile domains. The EBay or the Pay Pal or the Microsoft.com or dot whatever. It seems to me that if I were Microsoft and my name were transferred, I would probably have attorneys calling the registries as well as the registrar involved.

So (Barbara) are you saying in those circumstances you just put yourself at arms distance and let the registrars resolve it. And in something that exception based would you envision a registry, not necessarily (calm) taking a more proactive action?

Barbara Steele: You know obviously to channels on a case by case basis. And depending on the status of the name if you will and the level of attention it gets, you know that’s going to determine what actions we would take. And before we take any action on a name we would prefer to see a court order or some similar mechanism instructing us as to what to do with the name.

And from our perspective, we're a little different because we don’t have any visibility into registrant information, we would obviously reach out to the registrars to engage them to be, you know what they're doing on their end to try to validate the situation.

One of the things that we did do recently is we had submitted an (R Sep) application for a service that we call registry lock that we're looking at rolling out which would allow registrars to enter into a contract with us to submit their higher profile names for us to basically lock them down here at the registry and it would require any changes that we can control here at the registry the registrars would have to contact us and provide basically two (unintelligible) in order to unlock the name to allow any changes to occur to the name.

Dave PIscitello: I confess I was fishing for you to talk about that.

Barbara Steele: I'm not surprised. But, yes. I mean that it has been approved at the (R Sep) so we are looking at implementing that service.

Mike O'Conner: This is (Mikey). As soon as it's rolled out somebody please email me. I'd like to sign up for that.

Barbara Steele: I'll keep you posted (Mikey).

Mike O'Conner: Thanks a lot.

Barbara Steele: Sure.

Tim Ruiz This is Tim. I'd like to make a comment on that.

Michele Neylon: Go ahead Tim

Tim Ruiz: Yes I think what (Barbara) just describe in that (R Sep) (unintelligible) personally I think that’s an excellent idea and because actually some of the registries are doing that already but its kind of a little bit of an (ad hot) process and so this will at least kind of formalize that. And I think it's an excellent idea.

Of course that doesn’t completely solve some of the problems because on the registrars end there's still, you know I think we still need to discuss how can, what can the registrar do to ensure that when they're making that request they've done (unintelligible) necessary to make sure that what they're asking is appropriate. You know that somebody should talk about the identity of the registrant and those kinds of things will still be important.

Mike O'Conner: This is (Mikey). I want to chime in on that because I think what we're probably going to find the most difficult cases to deal with are the less prominent domains, sort of the small business person who isn’t very sophisticated, doesn’t have very good security and finding the balance between their culpability as opposed to a process change that we can make.

Tim Ruiz: Yes this is (Tim) here. I'd agree with that too. I think that while you know some of these high profile cases like (Antex) for example or whatever, while you know the total dollar value of what's at risk or the total (unintelligible) cause is very painful, I think that with some of the smaller customers that it could potentially be devastating even though the dollar amount of the total harm might quantify much less, the overall harm done to that individual could be totally devastating.

So ideally having a process that secures things better for everyone I think is important. But certain high profile sites I think will be clearly might be, you know some different factors that could come into play there or used for those. But your right we shouldn’t forget about the average user.

Michele Neylon:Just taking off my hat as the Chair here. I would be very much in favor of policies that benefit everybody, not just a select few. I mean with the example of Microsoft is perfect. Microsoft is economically in a position to hire a massive team of lawyers. Microsoft is in a position to have dedicated staff to look after whatever domains they may have to deal with.

And your average SME which in my term in our terms would be with less, with fewer then about 100 staff isn’t going to have that opportunity, yes if something were to happen to their domain name that could be completely disastrous to them. And in the grand scheme of things, could have a much more negative impact on them, on their business then the impact that EBay might feel if they lost control of their domain for two hours.

I mean for that small business, I mean the fear that I would have is that a lot of these reports talk about these very high profile cases but the reality is that a lot of the high profile companies are in a better position to take measures to secure their domains compared to your normal average user who's paying Go Daddy or (Enom) or who ever less then $10 a year for a domain name. So I think people should keep that in focus. Just my person comment. (Dave) go ahead.

Dave Piscitello: Yes, I have actually have to leave in about 10 minutes for another call but I just wanted to ask a questions if I might about the report dated 15 May, 2009 that Marika forwarded to me.

There's a section on 2.4 that talks about the (S Sac) 2005 report and then it goes onto some possible elements as an urgent restoration. I think that these are actually still relevant and (S Sac) would still be very satisfied if this were the direction that this working group would take and in particular the discussion about the policy to the action channel and the kinds of information that is provided here.

And what I want to do is encourage those registrars who and members of this group who haven't had an opportunity to look at the accelerated suspension work from the APWG to sort of look at that for some other models for what kind of information is appropriate. Who would collect it? Maybe establishing some criteria for magnitude of form.

And I think that this is all heading in what I would, what I personally believe is that is a very positive direction because there are two essential components here. You want as much collaborating information as possible and someone that you trust providing that information to further reinforce the confidence that the action your taking is appropriate.

And I think if you can model a response around those two first principles you probably will have a resolution process an urgent resolution process that would work in a very large percentage of the cases with a very small incidence of false-positives. If you compliment that with some kind of safe harbor from liability, because the registrars are acting in good faith, I think you have as good a response as any industry can possibly provide.

Michele Neylon: Okay, thanks (Dave). And Anil George you had your hand up.

Anil George: Michele I just wanted to say that I agree with your recent point that probably our focus should be on the community as a whole and we probably should not be sort of distracted by the fact that the parties involved in some of the reports may be very high profile entities. I think the issue is that this is probably a problem that can effect many different organizations.

Michele Neylon: Okay, thank you. Any other comments? No? Okay, (Dave) do you have to run off now?

Dave Piscitello: I have like five minutes. So I don't have to be precisely off at 11:00 but if there's something else that you want to ask.

Michele Neylon: One thing I was going to ask you about is based on the report. There was some mention about security regarding registrars and about some possible commonly accepted as standard, I think. It may have been mentioned at the (unintelligible). I mean are there any recognized such security certifications that the (S Sac) would recommend or ones that the (S Sac) would think are a total waste of time? Or is there anything in that area that you could talk to?

Dave Piscitello: Are you talking specifically about voluntary security auditing?

Michele Neylon: Yes.

Dave Piscitello: Okay. Well this is a (unintelligible) from the IRTT discussion but prior to being a member of (S Sac) and joining ICANN I was a street consultant and one of the groups of people that I would typically run into and either engage as part of a larger process where companies that did what are called risk and vulnerability assessments. Some time the (euphemism) penetration testing, you know what was applied to especially people who are one (off) companies, individuals with a high profile who were very, very skilled in figuring out how to break internet works.

That whole space has evolved to a much more sophisticated area of both software and service development. That ranges from web application testing all the way up to entire security auditing.

The idea that (S Sac) was establishing or promoting was one that sort of follows a trend. If a registrar decides that it wants to distinguish itself as providing better than average security measures for its customers, one of the things that it might want to do is go to a company like (A sound stone) or go to the (I Sacca) the independent security auditors, its isasca.org and look to see what they're criteria are and whom they actually use to, or what metrics they use to assess the security competency of an organization.

And so there's kind of an entire section of things you can do from having somebody simply scan your porthole to see if there are sequel insertions, vulnerabilities and exploits to having someone come in and do an onsite complete physical audit, complete business audit, complete operational audit where they look at all your systems. They look at your processes and your workflows and they try to expose where you might be exploited.

So they might conclude that you have locked solid hardware, but your staff is susceptible to social engineering. And the process has a flaw at this particular point in the workflow where there's an escalation because there's a hand off that’s not particularly clean with regard to the information past from first tier to second tier during the escalation process.

And those are quite extensive and I suspect at this point in time they are quite expensive but if your going into the, if your going to step up from being what everyone perceives to be a consumer oriented registrar to being a registrar that Fortune 100 companies should be willing to throw ten of thousands of dollars per domain at for security then that’s something you might want to consider.

Michele Neylon: Okay, thanks. Does anybody have any other comments or can we move onto the next item on the agenda? Okay, I'll take that as a no then. Okay. The next item on the agenda, and I've now ended up in Window, I have Windows Oracle all around me and I have no idea where I am.

Okay. The public comment announcement. Marika, do you have anything to say about that?

Marika Konings: Yes, I posted a first draft to the mailing list I think last week. And there hasn’t been any comments or any suggestions I think on the mailing list. I don’t know if that’s because people haven’t had a chance to look at it or whether they are fine with the text as is. So the question is do people need some more time to review and make edits or suggestions on the mailing list or are now on the call? Or are people fine the text as it currently stands?

Michele Neylon: Well I'll be honest and say I can't recall reading it. So I would say I would have to look at it again. Has anybody else got anything to say about the document that Marika sent around?

Mike O'Conner: This is (Mikey). I read it and thought it was fine.

Michele Neylon: How was the language? Was the language very clear and understandable for normal people or was it very jargon laid?

Mike O'Conner: IRPP is sort by its nature going to be a bit jargon (unintelligible) and given that caveat I thought it was fine.

Michele Neylon: Okay. Does anybody else got any other comments for Marika?

Marika Konings: And Michele what I can suggest is maybe research related to the list and give everyone till Friday to provide any edits or comments and then have the public forum opened on Monday if there are no major changes? Does that work for everyone?

Michele Neylon: I like that idea. Anybody have any comments on that idea? No? Okay. So Marika if you wouldn't mind resending that please. And the constituency statement template, did you send around a draft on that already or?

Marika Konings: I think that was enclosed in the same email. And I should presume that the same applies to that one. So I'm happy to recirculation that and.

Michele Neylon: Send it as a separate email if you wouldn't mind because I think if the way I handle mail is probably similar to what other people, if you send me two attachments I'm likely to read one not the second one.

Marika Konings Okay, I'll send them in two separate emails and I think probably the bigger question on the constituency statement template is due, do people want to ask more detailed questions or sub-questions to the charter questions to the constituency or do they feel that its fine with just putting the charter questions out there and have constituencies add information as they see appropriate, you know that we might not be asking for but they see relevant for the discussion.

Mike O'Conner: This is (Mikey). I sort of like in this first rounds to throw as broad a net as possible, as sort of an information gathering round. So I would lobby for open ended questions where ever we can. That’s not something I feel super strongly about, it's just find most useful on.

Michele Neylon: Any other comments? Anybody else want anything else from us?

Marika Konings: So Again I can resend that and you know people have until the next call to provide any comments. And then maybe on the next call we can decide to send it out and because I think it will give constituencies anyway some time to look at these and come back to us.

Michele Neylon: Okay. Now the definitions and concepts, I think I saw some emails about that earlier today though I have been very bold today in mixing up mailing lists. So I think I sent an entire group of people the wrong email.

(Mikey) were you sending stuff about definitions (unintelligible)?

Mike O'Conner: This is (Mikey). I did although I confess that was from a very old thread. And I'm not sure that was sent.

Marika Konings: That was a different (unintelligible) working group.

Mike O'Conner: Yes that was the other group.

Marika Konings: Pull up the email on the Abode Connected, it's (James) that has launched a discussion or put up a first suggestion and I think there have been some responses to that. But probably (James) is in a better position to summarize and indicate where changes might be required following the feedback received on the mailing list.

Michele Neylon: (James)?

James Bladel: Thanks Marika and Michele. So based on what are my take aways from our previous call was to try and put some language around some various concepts or types of transaction and some of these are often mistakenly referred to as transfers when in fact they are (unintelligible) distinct and separate operations.

There's been a few responses on the list, mostly clarification questions. So I don’t know that these definitions or at least these proposed definitions have been changed or modified significantly since they were originally posted.

But I didn’t know if you wanted to go through these now (Mikale) or if you just wanted to?

Michele Neylon:Well how are people doing for time? I mean this is obviously the other question I'd have to ask. I mean are we all okay for time?

Barbara Steele: This is Barbara. I'm going to actually have to jump off here in a minute.

Michele Neylon: Okay.

Man: Yes, I had expected the call to run about an hour.

Michele Neylon: Okay. Look maybe we can just try to be a little bit more diligent in following up on emails that (James) sent since the list then I suppose.

And yes I admit I have sinned as well. And (James) if you want to, you put up, I think Marika has put up that email that you sent around about your shop or customer registrant and everything else, I mean if people want to have a look over what (James) has done so far and if anybody has any input to share with the list. Olof you had your hand up.

Olof Nordling: That wasn’t particularly regarding one of the definitions and this a detailed comment. I would like to see some direct to reference to registered name (unintelligible) that the definition of customers. But I can take that on the list.

Michele Neylon: Yes if you wouldn’t mind Olof, sorry it's probably easier to thrash these things out in writing in some respects. What was the last thing there? The on the agenda as well, Marika the (Seoul) thing. Where are we at with that?

Marika Konings: Just most of you confirmed that you would be either participating remotely or on site, so my suggestion would be to go ahead with the purposed meeting time which is Monday Morning local time at 7:00. So we can take advantage of having a broader community there and, you know the group might want to through out specific questions or just have, you know a normal working group meeting and allow for the last half of the meeting for discussion and an open debate.

I mean the group can decide how they would like to use that meeting closer to the time.

Michele Neylon: So what time of the day did we end up with?

Marika Konings: Monday morning at 7:00. Breakfast will be provided included strong coffee.

Michele Neylon: Okay, as long as there's strong coffee for me. Okay, so stupidly early in the morning and so. Okay.

Marika Konings: (unintelligible) anyway so, morning, evening, you know.

Michele Neylon: You might be jet lagged, I'll probably be hung over.

Marika Konings: Well it gives you the same sensation.

Michele Neylon: No comment, no comment. I beg your pardon?

Man: One of those may be cheaper.

Michele Neylon: Olof you have your hand up again.

Olof Nordling: Oh no I should have lowered it, sorry for that.

Michele Neylon: That’s okay, that’s okay. I also have the same problem with it I keep forgetting. (Tim)?

Tim Ruiz: Yes just a couple of things I thought maybe that might be helpful to have on the wiki. One for perhaps the issue (A) we could include a link for that (S Sac) report 40. So that we'd all have an easy way to access that for reference and others who may come into the group later, it would make it easier for them to get familiar.

The other thing I thought I'd mention is just there's another report (S Sac) 38 or SACO 38 and you might also want to consider in link too. It talks about (abuse) contacts for registrars and I think that’s going to be something we'll probably end up discussing at some point potentially. So I would suggest at least that maybe the group review that.

The new RAA actually requires a contact be published on registrars website, this goes into a little bit more in depth about 24/7 contacts for abuse purposes and the reasons for that etcetera. So they're talking about quick resolution of some of these problems. That might be something that (unintelligible) want to discuss.

Michele Neylon: Okay, thank you.

Marika Konings: This is Marika. The link to the (S Sac) 40 report is already there but I'll create a separate section on something like useful documents or documents for review and include as well the (S Sac) 38 there.

Tim Ruiz: Okay, okay thank you.

Michele Neylon: If there's other things as well, I mean if there's other people who you feel should be part of the working group I've been trying to encourage people who are going to actually participate to join. So I think I saw at least one other registrar expressing an interest earlier today.

Does anybody else got anything else to add at this time?

Marika Konings: Maybe that the next meeting will be in two weeks as discussed on the last call.

Michele Neylon: Yes perfect.

Marika Konings: The 16 of September.

Michele Neylon: Okay. And if nobody has got anything else to add, I'd just like to say thanks again to Marika and other ICANN staff. (unintelligible) Hand up, go ahead (Michael).

(Michael Colins):I'll be brief. Is there a link to the email communications, a single place that we can review the email?

Marika Konings: Yes there are. If you go to the (GNSO) Home Page, there's on the left-hand side, I think a link called Mailing List Archives and there you should be able to find the (ROTP part B) archives. There's also a link on the Wikia, I think and if not I'll definitely post it there as well.

(Michael Colins) I was looking on the Wikia, I didn’t see it, I would ask you to post it there if you would please. If I missed it that’s fine, thank you.

Paul Diaz: Hey Michele and (Michael), its (Paul). I just put the link to the archive on our this Adobe site.

Michele Neylon: Okay, then so if there's nothing further. Marika is going to post a couple of those documents to the list. And if anybody wants to rip (James)'s list of definitions to shreds, please do so the list.

Okay, then. So thanks for everybody and I'll speak, we'll speak all again in two weeks time.

Man: Thanks Michele great call.

END