RECORDED VOICE: This meeting is now being recorded.

LAUREEN KAPIN: Okay. So we're going to get started. We're adjusting our schedule a little bit to allow for Brian to get through more of the very helpful document. We're going to do this for the next 60 minutes or so, and then we will move on to presentations, because we have two hours segment here, so we'll split it in half and move on from there. So take it away, Brian.

BRIAN AITCHISON: Great. Thanks. So I think we should just jump right back into this. Are there any questions or comments before I get started on this approach? Anything to include?

Okay, great. Okay, so now we're moving into these spec 11 slash GAC advice, or safeguards emerging from GAC advice, some represented within spec 11, and how to measure each. So, jumping right in, the first safeguard we'll want to look at is a requirement to use registrars under the 2013 RAA.

In my notes, I have an underlining question that this is essentially asking is, the 2013 RAA effective in terms of the safeguards it provides, that's my interpretation of it, which could be something of a hot potato, as I've indicated there. But I've flagged this as a kind of qualitative study, again falling into some kind of perception of effectiveness survey or questionnaire.

Does anybody have any thoughts on that? I think it's an important topic. I've flagged this as a sort of high bang for buck if we hired a vendor, or chose to focus on it.

Carlos?

CARLOS RAUL GUTIERREZ: I'm not sure that what I'm going to ask makes sense. There were no changes to the 2013 agreement, or the new end of signing new agreements. I'm bothered by the date, the 2013. You see, that was a version that existed before the new gTLDs were delegated. Laureen…?

LAUREEN KAPIN: …a little bit. So, before, and staff can jump in in case I am wrong. There was a prior version of the registrar agreement. I think the last version before this was 2009. Of the 2013 agreement, contained additional and different provisions that included numerous safeguards. And then there was a requirement for any registrar who was going to, anyone who was going to have a new gTLD, that they would have to be bound by this agreement.

And I think it's the registry agreement. It's the registrar, okay. So, this is the agreement that in fact, was required for new gTLDs registrars. So that's why it's being looked at, because prior to that time, this wasn't the key agreement. Karen, jump in if I'm misconstruing it.

KAREN LENTZ: Thank you. This is Karen Lentz. So the ICANN accredited registrars, all have this exact same agreement, and that periodically gets updated and renegotiated. And so, Laureen is correct. The last version that we had prior to new gTLDs was 2009. There was an effort already underway to update the registry RAA on, you know, the sort of usual process.

And at some point during the new gTLD program development, you know, there were [inaudible] to the effect that, you know, one of the things that would help, maybe address some of the concerns about expanding the space, would be to apply these extra requirements to the registrars, who would be selling new gTLDs.

And then, you know, to the question that Brian is raising, I think is correct that what you're, part of what you're asking here is the 2013 RAA effective? And I think that question is, you know, in itself out of scope for this group. I think looking at, you know, did including that, as a requirement, for the new gTLD space, does that make an appreciable difference, as opposed to what would have been required of all of those registrars under the previous RAA.

BRIAN AICHISON: Thank you. Drew?

DREW BAGLEY: Yeah, I was just going to comment on that. But the parts that might be relevant, at least for context, the 2013 RAA would be section 3.18, which requires that registrars undertake a reasonable investigation into abuse complaints, instead of waiting until law enforcement makes a

formal request. And so different interpretations of that can lead to different anti-abuse policies, and methods, and responses. And so that might be something on the tail end, when we're analyzing the data, we want to just kind of point to, or maybe even bring up any of the other categories in which we're actually holding focus groups with registrars, to understand their interpretation of that requirement.

And then, 3.7.8…

BRIAN AITCHISON: 3.7, okay.

DREW BAGLEY: Which would be the, which we already discussed that that will be the WHOIS accuracy validation…

BRIAN AITCHISON: Okay. Carlos?

CARLOS RAUL GUTIERREZ: Thank you Brian, thank you Drew. So if I understand you right, we don't want to know if they sign it, everybody has to sign it. The question is, how many cases do we have of 3.7 and 3.18? Is it right?

DREW BAGLEY: This is Drew again for the record. Yeah, and I mean, there might, there could be interesting compliance data if there had been complaints filed

against registrars for not following the 2013 RAA. So we would be interested in those. But to Karen's point, we don't want to get too lost in the weeds with the 2013 RAA for your exact point, because there are required to sign it.

But yeah, I think they would want to know if there were complaints overall about this, and then I think these two key provisions tie into other safeguards, and so that's where we would, at least, want to understand whether or not there is different interpretations of those requirements.

BRIAN AITCHISON: Okay. So it sounds like, it would be more useful to do, conduct the study for context more than sort of an effectiveness, sort of higher vendor and survey people kind of thing. Is that, are people generally onboard? Laureen?

LAUREEN KAPIN: Yeah, because… This is Laureen for the record. I think it would be very difficult to ask this general question, was this effective because it has so many provisions, so many provisions are different than the prior version, so I agree with you that it would be better to zero in on particular provisions, because otherwise, I wouldn't know how you would even, and I'm not a study expert, but I don't even know how you would control for the fact of well, was it effective because of this provision? Or was it effective because of that provision?

And it would all have to be, of course, compared then to the RAA that was in effect prior. So it becomes very… Yeah, it becomes a beast. Thank you. That's a good way to put it. So I think really we need to focus. And then again, for this one, you have to figure out who your target audience is to ask about effectiveness.

Is it about…? You know, is it, you know, IP enforces? Is it law enforcement? Is it the registrar community? Is it internet uses? So, you know, depending on who you ask, you can get very different answers. So I just think we need to consider those questions. Say it again?

[SPEAKER OFF MICROPHONE]

No, I didn't say that. I'm saying that it just depends… You will get a different answer to the question of whether it was effective depending on what group you ask.

DAVID TAYLOR: …following the rules, David. Hi, sorry. David Taylor. So compliant here. No, I just fully agree with us having to look into the 2013 RAA be a beast, which we honestly want to stay well clear of. I just want to pick up on your point, that's an interesting [inaudible] on the anti-abuse, excuse me, policies of registrars. I'm just wondering how we'd look at that with thousand plus registrars, and how we can get anything meaningful, but I'm not saying not to do it. I'm just trying to figure out what the next step will be on that.

[SPEAKER OFF MICROPHONE]

Yeah, with the registrar's policy because obviously they may or may not differ, but how do we go around doing that, and is that maybe just a bridge too far for us?

UNKNOWN SPEAKER: Sorry, sorry, it's getting into that kind of beastly nature of the safeguard, and it becomes almost an entire study in of itself, I would imagine. You can probably write a report on it. Ideas? Laureen.

LAUREEN KAPIN: You know, what I see as a general challenge, in that Brian's very useful exercise brings home to me is that, as Fiona said, we are not going to be able to do everything at this juncture. And really, one of our main tasks is going to be prioritizing what we can do now in the most effective way. So we may not be able to get at a study and information, and recommendations on each and every one of these safeguards.

So what I would ask people to think about, as homework, because as you all know, I love giving you all homework, and I know you love me for it. But what we should all think about as homework is really taking a hard look at how we are going to prioritize this, given our limited time and limited resources. What is really important?

Brian has done a comprehensive look at all of the safeguards, but that doesn't necessarily mean that we are going to be able to delve into each and every one, gathered data on each and every one, and make recommendations on each and every one. We're going to have to be targeted, smart, and efficient on how we do it. So I'm just putting that

out there, so we can get the benefit of people's views on what are our priorities. What is really important here for this first look, you know, by our review team?

There will be other review teams who are going to look at this. They're going to have more data, it will be at a different point in time, but we're the first. So what's really important?

[SPEAKER OFF MICROPHONE]

Feel free to respond.

CARLTON SAMUELS: All right. Carlton for the record. In my view, we look at… To me, what we are doing here is most like with this, there is no safeguards and measurements. It's clean slate. We're just building something. So I would recognize and I agree with you, we should prioritize. We should prioritize around the ones that we have credible means of getting data, because we want to be, evidence this in all our things.

And even the ones that we think would be useful in getting data for us, even if we don't have data now for them, we should at least make sure that they are included in that list. And we tell them we just don't have the data. So I would error on the side of prioritizing those we have credible means of getting to the data and assessing the data.

And the ones that even if we don't have data now, we should at least recognize them as important to the evidence based response that we are projecting.

BRIAN AITCHISON: Great, thanks for that. Any other comments on… Oh, David, please.

DAVID TAYLOR: David Taylor here. I'm compliance, but no one listens. No I was just going to say, maybe on that point of getting data, we could ask the registrant stakeholder group, if we group this as a question with other things, to the [inaudible], they may have some of that data on abuse policies and difference between the registrars and any data still worthwhile having, even if it's minimal.

BRIAN AITCHISON: Okay, great, that's very helpful. Any other ideas on data sources or how to approach this? Okay. Let's move along to our next safeguards. This one is a bit of a bear too. Registry specific public interest commitments, which is emerging from question 18 of the applicant guidebook. Are we familiar with this at all? Or is this…? So okay, Karen, thank you.

KAREN LENTZ: This is Karen Lentz. So I just wanted to give some background on this one. You know, question 18 and the registry picks aren't necessarily related in… They're not the same thing. So, back when we were developing the applicant guidebook, there was some advice from the GAC to the effect of, you know, there should be some sort of cost benefit analysis incorporated into how the applications were being reviewed.

And rather than incorporate that type of, you know, evaluation and assessment into the actual evaluation, the decision was to put a question in the application that ask the applicants themselves to describe, you know, what is their mission purpose? Why are they applying? Why are they applying for that TLD?

And then it asks them about how they attempted to, you know, create benefit for public benefit for their users or the internet in general. And then things that they might do to minimize any social costs. And the goal is including those, that question, was to do a few things. One being to inform anybody that would be reviewing the applications for the purpose of deciding whether to file objection, whether they wanted to issue an early warning, or something like that.

So the question was primarily educational. It wasn't scored. It wasn't evaluated in terms of whether an applicant passed or not. It was more of an essay question. And the, you know, what the Board response to the GAC's comments on that was, that it would be sort of more relevant as an exercise at a later point, to look at the statements they've made as the applicant in terms of the application and looked at some of the sort of cost benefit discussions when you have some data about how the registry is using the TLD.

And then the point about the registry specific picks, you know, seemed to us, you know, germane in some ways, so you had an applicant writing something at the time they applied about what they intended to do with their TLD. In some cases, when the voluntary picks were introduced, the registry had an opportunity to make additional commitments, make additional public interest commitments.

And so, what they may have done in some cases, would be to take some of the things that they wrote about how they were going to, you know, create more benefit and actually make that a commitment a part of it, a part of its registry agreement. So you've got a set of TLDs, not all of them, but you have a set of TLDs that does have these voluntary commitments in their agreement.

And so, if you go back to the IAG that recommended metrics that Jonathan was describing this morning, they did have this metric included in their recommendations, which was to essentially look at, do a qualitative study, I think, were their words, to look at what the applicant is saying in question 18, and compare it with actual use of the TLD.

And so we've, you know, done a few iterations of trying to figure out how you could do that type of qualitative study. So Brian is going to talk about a couple of options. So if that helped, thanks.

BRIAN AITCHISON: Yes. Thank you Karen. Much better synopsis then I could have given. Yes, so essentially what we're doing is we're tasked with comparing their stated commitments in question 18 of the applicant guidebook, with essentially how well they've maintained those commitments in actual practice, in terms of how they use the TLD.

We… I'm sorry.

CARLTON SAMUELS: And what's happening if you find a difference? What happens if you find a difference to the dispute?

BRIAN AITCHISON: That's one of our issues is how meaningful the methods we've tried to use are. And we've done just some very preliminary research into, just to see what a possible way to measure how effective these have been, and that's simply entails reviewing a sample of responses to question 18, comparing that to what's stated on the TLD websites, and how much sort of similarity or difference there is.

Now of course, this raises the question of how meaningful that is because, are they just repeating what was said in the question 18, to sort of be consistent and look good? Does it demonstrate how they're actually committed to those picks? That, in of itself, would involve a much deeper study.

So we're a little bit at a loss for this one. It's not quite as easy as telling a vendor to take care of it. It's literally just a very difficult issue to measure without, you know, delving into the nitty gritty details of how a TLD is operated in interviewing people and sort of putting them on the spot with how they're committed to these picks. So that's the problem.

CARLTON SAMUELS: So let me go for the record, because I'm on the record as saying that there weren't some buckets of warm spit. And the reason for that is very clear, they were voluntary. You had no way of measuring them, because you're not committed to them. And even when you look at the

amendments, those are [inaudible]. Picks, safeguards, they are [inaudible] in the amendments to the registry agreements. Even if you found something, even if you found something wrong with it, and they say well there is a process.

You've got to go through mediation and arbitration, and what not. And let's assume that this has been in arbitration, you go to mediation and arbitration. There is a dispute. I say I'm going to do this, I say you didn't do it, so let me mediate. We can't agree. Let's arbitrate. We can't agree. You know what?

The picks are [inaudible], the picks are not part of the mediation arbitration framework. They are actually outside of it in the amendments. The process, they give you a process, and they are not in it. And we knew this from a long time ago, so I can tell you, I've [inaudible] too much time to run it in the At-Large…

I was on the ALAC at the time it came up. I read the thing and I said, there are too many outs here for everybody. Not worth a bucket of warm spit. Still not worth it.

LAUREEN KAPIN: So, I think you raised some important issues with the advocacy of the public interest commitments, how enforceable they are, and the whole public interest dispute resolution process, and whether that's even an effective method of enforcement, or whether it's just a lot of time, complexity, and effort that doesn't end up with a defined result.

So I think those are important issues. Separate and apart from that, with the issue, at least preliminary that Brian and Karen have identified, which is, is there a difference between what applicants for gTLDs said in their application, and what they're actually saying on their website?

And that's separate and apart from what they actually do in practice. I'm going to section that off because that is a real beast. But I would say just at a threshold level, maybe we could at least see if there is difference between the application and the public facing website. That might be something we can actually do and get information on, actual process maybe that is a lot more challenging and resource intensive, although it's more important actually, because of course, we care more about what people do rather than what we say they do.

But in terms of what we can actually study, maybe it's just that first part that we can actually study. And just as a placeholder, causing the whole issue of the picks and the dispute resolution process, that has been a big topic of GAC advice, which when we get to our reports on data sources, GAC advice, which is one we'll be focusing on a little more.

UNKNOWN SPEAKER: Yes, I think this is very important. And I can see three cases where this is relevant, when different people apply for the same community TLD, and it has not been assigned, okay. This is very important. The second one is when somebody who didn't get the domain name is an IRP against ICANN and is using these types of argument about IRP. And the third one is when the business model of the domain name fails, and somebody wants to buy it or to save it, and my [inaudible] argument

that he's going to change the purpose of the domain name or from the peeks where the barrier to success, he wants to take it over but use it differently. So I don't know how to deal with that at this stage, but having been in the GAC when this was discussed, this is a very relevant issue.

And the problem being that the semantics of public interest are still defined in ICANN as another level of complexity, because ICANN has promised the community to develop some semantics, let's say, on public interest. And the word has been used in the new bylaws, etc. etc. So, I'm not sure that shooting in the direction that you proposed right now, just comparing the webpage with the commitments is useful, it's a minimum, but this is certainly something we have to think about.

And if we don't solve this time, just make a note that we have to say, oh, we didn't solve this one. We're leaving it for the next review team, because this is very relevant.

CARLTON SAMUELS: Actually it's kind of relevant what Laureen says, because the first two mentions that you propose, that was what the discussion was in the At-Large. There were a couple of the applicants who made commitments, and then if you look at what came out on the website, there was this distance between them. To me, having that figure as a baseline, is very important.

I mean, I know that, I like to ask… A couple of them did some checks, and I know Garth and Evan were very much involved in doing the checks. And there is a document somewhere in circulation, in the At-

Large, with some of that data. A very small set, but if they were used as arguments for why it was important to have a more robust enforcement element with regard to the picks.

So I actually endorse doing that top level look, Laureen, and just look at what they said in the application, look at what they had published subsequently.

BRIAN AITCHISON: This is Brian for the record. I mean, I think this is a very useful discussion just to get your sort of personal insights into the processes is in of itself an insight into the advocacy of the program. And I think that might make this study a candidate for sort of some interview based kind of studies, pulling people aside to discuss just those kinds of things that you talked about.

So I will flag that as a potential method. Karen?

KAREN LENTZ: Thanks Brian. Karen Lentz. This is just, again, to kind of clarify the terms. When we're… We were talking about question 18, these aren't commitments. These are looking at the applicant's responses at the time they applied versus a future operation. And I think I'm going to suggest that we actually try to make this two lines.

Like one on question 18 that respond to that metric and the second one on picks themselves. And then if you do the research on both, then you can look at synergies between them. And for the second point, I think Carlton's pointing out, there is a lot you can look at. You've got a

smaller set of registries that have picks, and then you have the GRP and complaints and, you know, other ways of looking at the effectiveness of the pick approach. Thanks.

BRIAN AITCHISON: Okay. Great. Okay, any other comments on this? And I'll have to [inaudible] before we can reach a conclusion.

UNKNOWN SPEAKER: Yes, I mean there is the GNSO is in a discussion with the Board on the follow-up, and definitions, and so on. And letters are exchanged regularly, so there is a very close follow-up of who is going to make the definition of the public interest. If it's going to be the executive, it's going to require policy development and so on. So you can be sure that there are some stakeholders before the…

Just the issue of the responsibility of public interest, very closely. So you have to include or mention that this is a parallel courses.

BRIAN AITCHISON: Okay. Great. Okay, to move along. These next two, next three, all of them, but let's just focus on the next two. We might just need to put a pin in, or that's my initial thinking. So we have included within spec 11, a prohibition of abusive activities, [inaudible] phishing, malware, these kinds of malicious conduct activities that we're all aware of.

Following that, there was a provision that the registries has to conduct a periodic statistical analysis of security threats. The standards for those

analysis have not been developed. There is not really much to measure there in that sense. Also the prohibition of abusive activities, it seems like it's just kind of saying don't be a bad guy, be good.

Again, I would probably throw that in maybe a vendor perception of effectiveness bucket, but I'm at a loss hung on these two. So Carlos.

CARLOS RAUL GUTIERREZ: Yes. This sounds very similar to a segment of five or six questions on these issues in the IG or, I don't know, I always get it wrong. But IAG, IAG, there is this specific section of IAG asking for very close follow-up of the reports of this type of incidents. So whoever does it internally or externally, I have no opinion, but it should converge with that.

BRIAN AITCHISON: Okay. So, my sense of this is, should we kind of put a pin in these for now? And just say that we were waiting development of these reporting standards before we can really study it effectively and provide it some kind of description?

CARLOS RAUL GUTIERREZ: In this case, we're also responsible for the others, so I think we can do it for the very short term, but we cannot go out in three months with that explanation, because we are also, it's part of our duty to see implementation of this indicators and so on. So in this case, it's totally internal, we have to find a solution before we write something public.

BRIAN AITCHISON: Okay. So it comes down to… Karen, go ahead.

KAREN LENTZ: Thanks. This is Karen. I think maybe there are two things we're interested here, looking at specification 11. So you know, the first is obviously what are the levels of activity that this is trying to guard against, phishing, malware, etc. So we've talked about that already, looking at you know, what information we can glean about the [inaudible] of those things.

But the provision in spec 11, I think that we're talking about, is talking about the registry including in its agreement with registrars, a requirement that the registrar must include this provision in its agreement with registrants, right? So I think, you know, part of what you're looking at on one level here is, you know, has there been an impact on those activities because of the requirement that this specific provision be included in the registration agreement where, as opposed to, you know, the terms that a registrant would have agreed to before, which strikes me as very difficult to study.

You know, there is one piece of this that we're obviously interested in, which is the ways of these types of abusive activities at this point, as regards to this safeguard in spec 11 is the effectiveness of having this requirement to include this specific language.

CARLOS RAUL GUTIERREZ: Karen, please, I need clarification. By including it, the registrars are supposed then to produce the reports, and then avoid this situation that

Jordan mentioned, they don't give us any data, so we will have monthly reports, or yearly reports, from the registrars. So it's not only putting it in the contract and signing it, but then complying at least writing we have no incidents, even if it's a lie, or not.

KAREN LENTZ: So in terms of the registrar requirement, are you talking about what's in the RAA? The new RAA to report, or…?

CARLOS RAUL GUTIERREZ: [OFF MICROPHONE]

KAREN LENTZ: Okay, yeah, that makes sense. That's not what I'm looking at in terms of spec 11. So it's, yeah, so it's another point that you could note, yeah. And then the, you know, also in spec 11, which is probably the next thing is about the registry, which does have to conduct this analysis of behavior of activities in each TLD and for [inaudible] reports, and as I mentioned, the framework for that reporting is still being discussed, I think.

BRIAN AITCHISON: So, sometimes I like to reduce things for simplicity's sake. There seems to be still a fundamental question in terms of ethicacy that needs to be asked. Did this prohibition of abusive activities have some kind of marked effect on the DNS abuse rate? Which seems a bit of, not a silly question, I mean, it's an important question, but it's kind of like asking,

does making bank robberies illegal decrease the amount of bank robberies?

I mean, I'm not… It's one of those things that it comes down to a deterrent effect. Is this having some kind of deterrent effect because there is language in the agreement? I'm not supposed to be a bad person, but I wasn't aware before the 3A spec 11. Carlos?

CARLOS RAUL GUTIERREZ: If in one jurisdiction, the law enforcement agency comes and takes the site down, then yes. Does it apply to the whole domain name? No because it's generic. It's all across the world, and so, but if it's enough for one judge in one place, even Pakistan, whatever, to say okay, there is grounds because suppose they signed an agreement with ICANN that they wouldn't do it, but they did it. Take it down.

I mean, Brazil, they did the other day with What's Up. And What's Up is not a domain name, it's an application, but if it happens, then there is a good argument for the judge, even if he doesn't know much about that, if he would get the information from somebody complaining. Listen, this guy signed an agreement with ICANN, he would, he did it.

And then they take it down, there is the result, very difficult to follow-up, I agree. Very far away from the responsibilities and the remit of ICANN, but yes, it's relevant, I see it coming.

LAUREEN KAPIN: So to me, the key question for us is how do we measure this? You know, Carlos, your point… I mean.

[SPEAKER OFF MICROPHONE]

Okay. Yeah.

[SPEAKER OFF MICROPHONE]

Right, and I think we all can come up with intuitive, you know, as Carlos did, what would be the benefit here? But if we're going to want to have the heft of some data behind it, I think we're still safe with the question of how do we measure this? And I'm not sure I've heard a great answer to that yet.

I think it's a very complicated question.

Well no, I'm going to disagree there because, I mean, just from a law enforcement perspective, I'm not going to take something down because someone has violated a private contact. ICANN is in charge of enforcing its contracts, as law enforcement, I'm going to take something down because there is evidence, and a law has been violated.

That's how a government agency is going to work. The fact there is contracts that have been violated, that's not my purview as a government agency. That's for the parties to the contract to deal with, with each other. So I would disagree that that's going to be something we can really look at.

In terms of deterrence, you know, that's a different question. Is this a deterrent? Are people more deterred because of the contract? Are people more app to behave in a legal manner or, you know, worthy manner because of it? That's a different question.

BRIAN AITCHISON: All right. Calvin?

CALVIN BROWNE: You know, I want to see the take down reports. And take downs don't really take apply to domain names to match its content and web hosting, as opposed to registrars and registries. So, to link the two together, to link content with the actual domain name, is going to get into something where there isn't a cause and effect there.

BRIAN AITCHISON: Okay. And just in the interest of time, I'm going to sort of move us along. We'll just, you know, sleep on this and think about it. We're going to come back to this, so maybe some great ideas will come to us. So I keep a notepad by my bed. That's usually when my ideas come to me.

Okay, so here is a bit of a similar kind of safeguard, but it was a requirement to operate a TLD in a transparent manner. Not easy to measure any of that, what is transparent? Is it being followed? Is it being followed as a result of the safeguard being included as a safeguard?

Again, it's kind of… My early thinking was essentially zero sum phenomena, it's either there or it's not, and we have to find some way to define transparency. Does anyone know, are there any sort of definitions for what that means to operate the TLD in a transparent manner? Is that…? Karen? Thanks.

KAREN LENTZ: Well just to read the full text of that provision. They'll operate the TLD in a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing, and adhering to clear registration policies. So there is a little bit, I mean, you've got some more judgments there about what's clear or adhere to.

But you can at least check that there is a registration policy, and that it is available to people, the public, on their website. So that's one aspect of it.

FABRO STEIBEL: Fabro here. For transparency, we can consider three criteria. The first one is information is somehow public at some stage, not all stage, but some stage is public. The second one is public participation, that at some stage, all of the stakeholders can comment and participate, somehow. And the third one on accountability. There are at some stage, mechanisms for people to criticize on that, and some public [inaudible] processes.

So there are three ones, transparency, participation, and accountability is achieved, it would be…

BRIAN AITCHISON: Great. Did you have that written down, because that was very, it was perfect.

FABRO STEIBEL: [Inaudible] open partnership in Brazil, so these are the criteria. I'll send you all the [inaudible].

BRIAN AITCHISON: Okay, great. Thanks for that.

LAUREEN KAPIN: So, just a quick response. I really appreciate what you said Fabro, that those are all three very important criteria, but I do wonder if the accountability and the sort of ability to comment go to transparency, or go to something else, they're very important, but I'm not sure it's transparency. So I just, you know, reflect that observation. That when we're talking about transparency, the visibility, do I know about it? Not whether I could comment on it and whether they'll change it if I make them aware of it.

That's very important, and I think that to me, is accountability but not necessarily transparency.

FABRO STEIBEL: Yeah. Fabro here. Good point. The one thing we can use in the literature review, there is an analysis of how many people access the ICANN website. So maybe for the, when you give transparency, so when you put online how much views you've had, so maybe we have some analytics or how many times this process access by others, then the stakeholders applying for the process itself maybe.

[SPEAKER OFF MICROPHONE]

BRIAN AITCHISON: Good ideas. This is Brian again. Any other comments on this in terms of method? I think we might have to delve a bit deeper before we start thinking about methods. Okay. So, moving along, we have another safeguard. No exclusive registration criteria for generic TLD strings. This is emerging from GAC category two advice.

I've seen this as another qualitative study. It does seem again, a bit of a zero sum question, just for a bit of context. In the application process, those applications that did drop, they were required to drop exclusive registration policies. If they wanted to proceed with the application. 184 out of 186 did, and the others were deferred to a next round.

I have to admit, I'm not very familiar with the safeguards, but so I will defer to anyone who may be in terms of how to measure their ideas. Laureen?

LAUREEN KAPIN: So, this, as I understand it, this really is, to me, bears on competition issues rather than consumer trust issues, because again, as I understand it and that's my caveat, this deals with whether a generic name like say, I'll just pluck out, let's day dot dog, okay? If it's a sort of generic name like that, the GAC advised… So these generic names, we don't want people saying just owners of Pekinese Dogs can apply, or just owners of pedigreed dogs can apply.

We want everyone to be able to, if they want to buy a dot dog domain, and that to me, it's really a competition issue that you shouldn't have to

have restrictions on who can scoop up these generic domains. And that's such, I'd say, is called outside of what we're looking at. Yes, it's a safeguard, but it's not a consumer trust safeguard, as I'm understanding it.

[SPEAKER OFF MICROPHONE]

BRIAN AITCHISON: Well, it's, that's great. If we could eliminate these and, you know, pass it over to the other team, then I'm all for that. Does anybody disagree with that assessment or have another idea on it? Okay, good.

Now, we have GAC category one safeguards. I think we might be more familiar with this. Essentially, actually, I have them… Let me change my view here. I think… Okay, well they must have disappeared. There they are. Can we see these? That's probably… See if I can zoom.

[SPEAKER OFF MICROPHONE]

Right. These are safeguards dealing with regulated, highly regulated sectors and some special safeguards. You can see a list of them here. So I've categorized one safeguard in the matrix, but you can see it's actually eight different safeguards. But a lot of them fall into this, don't be a bad guy, kind of safeguard. Comply with all applicable laws. Make sure that registrants know to comply with these provisions.

So some of the, I think, more interesting ones to perhaps focus on, would be registrants collecting sensitive financial help data, must secure that data properly. That might also fall into a discussion of, you know,

an HSZ framework, high security zone framework, if that doesn't confuse things.

For highly regulated sectors, they're to publish a point of contact to facilitate relationships with relevant regulatory bodies. Registrants need to provide contact information, and thus licenses for their sectors in which they're operating, and consult with authorities on credentials and, credential authenticity complaints and report updates and changes to credentials.

So I think there is a lot to study here, and a lot that's important. But is it, how do we see this as a priority? Laureen?

LAUREEN KAPIN: So I think that is actually, I think it's really important, but I also think it's really challenging because there was a lot of GAC safeguard advice given. Not all of that advice was accepted, and the credential advice of highly regulated sectors is… The best example of advice that was not accepted. So if it isn't accepted, how can you measure it?

At least on that point, there are some domains that have voluntarily restricted their registration policies in highly regulated sectors. Certainly that's something we can look at. But it's very important to understand that not all of this advice was actually taken. So it's not a requirement, and we need to be very, very precise in how we are describing the reality, so to speak.

Because we can't go forth and assume that all of these safeguards were actually implemented because many of them were not.

[SPEAKER OFF MICROPHONE]

BRIAN AITCHISON: The first step would be to ID which ones are being implemented.

LAUREEN KAPIN: Yes.

BRIAN AITCHISON: Okay. Okay, since we're running short on time, I'll just flag that. So again, think about it. Keep that notepad next to your bed. Okay. So now we're moving into rights protection safeguards. A bit of a different animal, and I again have to say, I'm not as familiar with these safeguards as I am with, say, the DNS abuse safeguards, but I know some in the room are.

So, let's just jump in. We have a trademark clearinghouse that was implemented as a safeguard. I flagged this as something we could perhaps survey people on, who have used the service and its [inaudible], let's open to [inaudible] on how to review the effectiveness of the trademark clearing house. Karen?

KAREN LENTZ: Thanks Brian. This is Karen Lentz. Just wanted to point a few data sources here. One is there is currently in process, an independent review of the trademark clearinghouse, which was something that was recommended by GAC about five years ago. So that's being undertaken

currently, and that includes, you know, looking at aspects of the clearinghouse and how it operates, as well as the sunrise and claims services, which is underneath there, which it supports.

So that's one thing. We expect that report to be available into three of this year, so July, August timeframe. And then, this second source here is, you know, one of the first sort of preparatory exercises we did for this review team was to compile the data that we had on the RPMs, and seek public comment on kind of the aspects that people believed were working well, and areas that perhaps could be improved.

So if you go back to the, what we call this RPM review report, it looks at, for example, you know, how many marks are in the clearinghouse, what different countries are they from. We know how many sunrise registration [inaudible] across the TLDs. So there is a lot of specific data points that you have that will go to a few, several, pretty much everything in this bucket.

You've got at least some initial data there to start with.

BRIAN AITCHISON: So, will this independent review, will this not just kind of tick that box? Can we just draw on that, the results from that?

KAREN LENTZ: Well, this is Karen Lentz. They're not being tasked to answer the question of, you know, was this effective at protecting rights in the program? You know, there are certain things that they are asked to look at, just matching rules. How long the claims service asked? And

certainly it will touch on, you know, pretty much everything that this group considers, most likely.

But that review is informational, so it's being done by a contractor analysis group, and they're not going to make recommendations as to what ICANN should or should not do in terms of just the trademark clearinghouse. So it gets to a lot of the information, but it doesn't really do the same job.

BRIAN AITCHISON: So my thinking is that, again, it might be useful to have a survey, just to survey the people who have used the trademark clearinghouse, and get an idea of the effectiveness through that method. There is any other ideas, of course, combined with what is produced in the TMCH report. So if there is any other ideas on that, I'll kind of flag that as discussed for now.

Carlos?

CARLOS RAUL GUTIERREZ: It's a question for Karen, because I don't know enough about this. I mean, I need a benchmark or a comparison like, okay, we do this, and we hope that by having you situated by clearinghouse, we will have less UDRPs in the future, or things like that. And then, I miss like contact with the pass or something like that. I don't know if it makes sense.

KAREN LENTZ: Thank you Carlos. This is Karen Lentz. The, it's a good question to look at sort of the initial goals of the clearing house, why people proposed it and why we implemented it. And you know, it was proposed by a stakeholder group called the IRT, that was looking specifically at how to you know, build some trademark protection into the program.

And some of the goals that they included in their report would be, for example, to create some efficiencies, so if I'm a trademark holder, you know, I used to have to go to, every time a new TLD started up and had a sunrise, I had to go prove my trademark all over again.

Sometimes provide one set of documents, sometimes provide a different set of documents. And so one of the things that the clearing house is intended to is to, you know, you go one place, you have your marks verified and then all you have to do is to sort of show your credential every time you go to register a sunrise name.

You know, so that's one aspect of it, you know, creating efficiency on the registry side too so that they don't have to do the checking of trademarks, and assessing whether they meet certain requirements or not, which could save them from costs. So the reciprocals, I don't know if David wants to elaborate, but you know, when looking at discussion of whether it was effective, it's really helpful to go back to the reasons that was initially proposed.

DAVID TAYLOR: So David Taylor. I won't elaborate too much, or else we won't have any time for anything else, so I agree with that. The only thing I would say is that it was interesting because right at the very beginning, one of the

big discussions is, should we make the trademark clearing house mandatory or not? And we were divided on that, I had a personal view and some thought yes and some thought no.

And I understand that that's kind of a fundamental questions for going forward, which will tie-in to whether we think it was worthwhile and whether it has been successful or not. So, the independent review is perfectly timed to Q3, so ideal. We couldn't have planned that better.

LAUREEN KAPIN: Okay. So we're getting to the end of our time. So maybe I can ask you to just conclude for now so we can turn over to our exploration of our readings.

BRIAN AITCHISON: Yeah, I think it will be good to take a break. I think it's hard to really think about all of this on the fly. So what I'll do is I'll polish this up, sort of and provide sort of a neat record of our recommendations, as far as we have them, and then if you could just read. There is a few more boxes, probably I would say about six, seven.

So maybe read through them and for now, just have a think about them, have them in the back of your mind, as to again, how to measure effectiveness, which is really what it all boils down to. So I appreciate your time on this, it's been incredibly helpful for me, to try to get my head around potential methods and I hope it has been helpful for you. So thanks very much.

LAUREEN KAPIN: Thank you Brian. This has been very, very helpful and I look forward to revisiting this. So, we're now going to change orientation. Alice, if I can ask you to put our Google spreadsheet. The next time we're scheduled to take a break is 3:45. So we're not going to take a break where we go outside now, but in the interest of clearing our heads, what I would say is that maybe we could all just stand up…

[Break and stretches, chattering]

Okay, so we're going to get back to our reading list. Just a show of hands, not to put people on the spot, but just to know who I can call on, who, in the room, has filled out the Google document reporting your findings? Who in the room has done that?

Okay. Not everything, that's fine. Okay, so we have a lot of people who have done it, that's great. For folks who haven't done it, I encourage you, strongly encourage to do that, so we can have the benefit of your findings on this document. But what I'd like to do is start off our presentations, and I think I'm going to do it just by person. Everyone has about five or six, or perhaps seven, articles that they were assigned.

Thanks to those of you who volunteered for your preferences, that makes my task a lot easier. And we'll just go person by person by person. So we're going to keep it short, but what I would really like to hear is, as Jonathan said, how your data source relates to the prism of our review team's focus, i.e. how your particular article relates to our task of thinking about whether the new gTLD program has had an effect on consumer trust.

So, is there someone who would like to start us off? Thank you Drew.

DREW BAGLEY: It's the least I could do after all of that Yoga. I'm feeling energized. This is Drew Bagley for the record. Yeah, I'll just run through the articles saying exactly that, the context of what should be applicable here with our research and our study. So the first one that I…

LAUREEN KAPIN: And maybe we could, whoever has ownership of the screen, maybe we can scroll down to Drew's section…

DREW BAGLEY: Yeah, if you want to do find, you could search for my name, otherwise the one I'm going to go over first would be the secure domain foundation report.

LAUREEN KAPIN: And for those who haven't put their findings in this document yet, what I encourage everyone to do is put their articles serially, i.e. you know, just find a place in the chart [CROSSTALK]…

DREW BAGLEY: …Jamie, Carlton, and then me, I think. I think I'm right under Carlton.

Getting close, that's not me, I did attribution.

LAUREEN KAPIN: That's the anonymous person.

DREW BAGLEY: There I am. All right, so yeah, so for the first article, the secure domain foundation report. What I found most applicable for us, and this was a survey based report that actually interviewed registrars, this is a bit of what I was referencing earlier. I thought it was interesting that the registrars differed from one another in how they interpreted their own responsibilities under the 2013 RAA.

And I thought that was what was most applicable for us. And so this would be a report we might be interested in finding for at least those purposes, because it demonstrates evidence of that. And what that interpretation leads to in practice is a difference in how different registrars deal with abuse reports, and what they're willing to do about anti-abuse in general, whether they're checking for bad things before it's reported for them, or whether they're waiting for a specific complaint to actually go ahead and do an investigation.

And when they do an investigation, what they're actually doing in terms of that investigation. Similarly, this report also describes a bit of the WHOIS verification and how that can differ from registrar to registrar and what they're doing for that. For the next one… Or does anybody have any questions about that?

Okay. For the next one, and the next couple deal a bit with similar topics. The next one was about amplified DDOS attacks, and…

LAUREEN KAPIN: And just, you know, for just explain terms just to make sure…

DREW BAGLEY: Sure. So amplified distributed denial service attack. And so, what this was, was this was an interview by ICANN's own Carlos Alverez, of cyber security experts, and was looking at ways to mitigate these types of attacks. So this is not necessarily directly applicable to the new gTLD program. However, what I thought was applicable… So therefore, this wouldn't necessarily be a resource we would cite in our report, but the main takeaway from this would be that we would want to, once we're doing that massive DNS abuse study, we'd want to look in there to see if new gTLD operators themselves for the registries have actually been affected by DDOS attacks.

Also what this would lead us to look into, as well as the subsequent reports that I'll go over, would be some of the DNSSEC issues and whether or not, what percentage of top level domains versus second level domains are DNSSEC signed. But this piece primarily dealt with things that ISPs could do as opposed to domain name registries.

Any questions on that one? Yes.

UNKNOWN SPEAKER: Thank you very much. I think it's very important what you said, that some of the documents here, we have to enjoy and keep in the back of our minds, but are really not related to the purpose of the report, particularly when they don't focus on DNS issues directly because that happened with two of my four papers. Thank you.

FABRO STEIBEL: Fabro for the record. Drew, one idea I had reading the [inaudible] is that there is a reputation from the registers, that for some is quite important. And any one connect, we heard from Nielson's review, user doesn't pay too much attention for that, usually trust the source. And they're trusting [inaudible] kind of regulator anti-virus program, software.

So maybe we can think of a way to give publicity for reputation of registrars in a more centralized way. It's not a metric we can use, but [inaudible] on how reputations of them are compared to charter. If I'm good, I'll say I'm good, but if I'm bad, I'll probably say nothing. So eventually, if you have a public record of reputation based on the metrics, might be a good way to enhance what they say are the increased costs, why you would do it, because it gets reputation. Just throwing ideas.

DREW BAGLEY: Yes, to respond to that, I think that's a very good point you brought up, and I kind of glossed, I didn't even mention that. But in that first report, that was one of the takeaways too from the surveys, was that registrars do care about their reputations, and that they even spend resources making sure that they're responding to bad things that are said about them in online forums or with the better business bureau and so on.

So along those lines of what you're suggesting, after we conduct this big study, I imagine we might have thoughts one way or another about what will ICANN security or ICANN compliance can play an ongoing studies of DNS abuse, particularly with regard to reputations for

purposes of seeing if there is a TLD operator that always has 90% bad domain names, and you know, that's always publicized so then the public is made aware of that consumer trust issue.

Because what happens anyway these days, is you can potentially get entire TLDs that are blocked if they're untrustworthy. So for example, the ccTLD dot SU for Soviet Union, you know, some recursive DNS operators will completely block that domain name, or dot CK is the other example from years past. And so, exactly what you're inferring could definitely come up in new gTLDs if they are known, a particular one is known to be bad.

FABRO STEIBEL: And one idea, what we can measure, when we're talking about it, spoke about privacy, and then one of the ideas was to survey how many registrars have the privacy policy in their websites or publically available. Maybe here, just throwing ideas, we can see how many registrars actually respond or have a room for public response to complain. Because they complain that one of the things that I read said that to file a complaint like on a website is really difficult.

Not saying I agree with that. But then ICANN is one venue for complaints, and then maybe [inaudible] playing the role as a complaining venue. So we can survey how many of them publically let people public comment on that, or have a link to send comments.

DREW BAGLEY: Those are some good ideas about ways in which the public could be educated on the reality, because what we were talking about this morning was perception, and then with our data, we're trying to get to the reality, and that might be a way to marry the two in the end. So I like your way of thinking.

The next report was an old one from 2005, next article. And there was a brief one on DNS cache poisoning. And so DNS cache poisoning can take place in a variety of ways. It could be on your local machine, and so that your machine is not truly querying the right IP address when you're typing in a domain name. So you're not being routed to the right domain name because the DNS cache on your computer has been corrupted, or just because potentially effect an actual DNS resolver.

And so what these issues, DOS or directly consumer trust, so if a consumer can't trust when they type www.icann.org into their browser, that it would truly go to the real ICANN website and that's a huge consumer trust issue. So this is something where I don't… Since this is a very old article, I did not deal at all with new gTLDs and I've not read enough yet to know if there are any issues that are specific, potentially specifically unique to new gTLDs as opposed to just all gTLDs.

And I couldn't think of any, but if anyone has any thoughts on anything that could be unique to new gTLDs in this area, then we should look into that.

Okay, and the next one was, the next report I read was the WHOIS accuracy reporting system, but there was a link to their webpage was on the reading list, so then I read the reports on there. There is a new

report forthcoming this month, and so that might be the one we would want to look at.

We talked about WHOIS accuracy already and how that, in of itself, is not going to be a beast that we are going to tackle, because there are initiatives such as this going on. But something that I've found to be interesting is that with all the talk we do, we have the 2013 RAA versus the 2009 RAA, 97% of domain names said they, as of last fall, were actually operating under the 2009 rules, due to the grandfathering mechanisms.

And so that was such a small data set of domain names actually operating under the 2013 RAA, and that would actually be worth looking at. And so we have that with, obviously, other areas too such as the similar number of 3% for the second level domain names that are signed with DNSSEC. But that's something where perhaps with the vendor data, Brian it would be good to hear your thoughts, maybe we would get the vendor to look at just that 3% slice, and see what we could draw in terms of the 3% of domain names that are actually under the 2013 RAA versus the whole other universe of domain names to see if there is any correlations we can draw.

BRIAN AITCHISON: This is Brian for the record. Could you sort of restate the question?

DREW BAGLEY: Yeah, I'm sorry. So this is dealing with WHOIS accuracy, which in of itself, we mentioned might not say something one way or another

about abuse. If the bad guy uses terrific syntax in an email address that works, and someone else's real address, then they're going to pass all of the qualifications with flying colors for the WHOIS requirements, but with that said, since this report does point out the fact that 97% of domain names today, even if they are new TLDs are somehow finding their way operating under the 2009 RAA, are suggesting that we could perhaps look at the 3% of domain names that are actually operating under the 2013 RAA.

As a little bit of, or little slice of WHOIS accuracy, perhaps, either way, we would want to wait until this June report comes out to see what's in that.

BRIAN AITCHISON: Yeah, just a general comment. I mean, I think segmentation is always a good approach, and I won't say any more than that, but yeah.

LAUREEN KAPIN: Drew, I'm looking at your next note here that there doesn't appear to be a difference in the 2009 RAA based accuracy of WHOIS data, over legacy new gTLD data. Do you mean there is not a difference in the requirements of the RAA? Or there is not a difference in the stats?

DREW BAGLEY: So this study only apply the 2009 metrics to the… Because of the fact that 97% of domain names run under the old rules, they only use old rules as the baseline for their study, and so then you applying the 2009 requirements, they were, there are such similarities between the two

classes of domain names, versus if you use the 2013 RAA metrics. I'm sure you'll come up with a different conclusion.

And for example, I actually looked back at the report itself, but I just didn't think it was relevant for our purposes, but you know, postal addresses maybe was lower in one than the other, but then email address was about the same or whatnot. So on the whole, I just didn't think this, the particular phase one and phase two reports were applicable to our study except for noting what a small percentage of our domain names actually are falling under the 2013 RAA.

If nobody has any other questions, I'll go on. The next thing, I don't have any notes for, is the entire list for RFCs. So I have not had a chance to read through them all to see what would be applicable to us, but I do want to take the time to do that. So I'll have to come back to that one. So the request for comment that have created all of these wonderful standards that we have today.

And so the link on the website went back to the entire index for all of them, yeah. Unless I look at the wrong link, my reading list.

No, I'm going to go through the index to see what might be applicable to safeguards, and then would skim them. I'm not going to read every RFC.

[SPEAKER OFF MICROPHONE]

LAUREEN KAPIN: So what I would say in general with our reading list, if something seems monumental and is perhaps questionable value given the time it would

take, then make a reasonable decision about what makes the most sense, for everyone, because I've gone through to some of these links also, and you know, [inaudible] surprise.

DREW BAGLEY: So the next one was the DNS stability, security, and resiliency report, and this definitely could be used as a primary source when we were looking at the DNSSEC adoption issues. However, I didn't categorize this in the traditional hypothesis research conclusions tabs, because I thought that was pretty much the applicability for our purposes.

[SPEAKER OFF MICROPHONE]

It's the ICANN one, and that's the exact title of it if you Google… I can paste the link into the box.

[SPEAKER OFF MICROPHONE]

Yeah, I don't have the document that has the URL up, so I apologize for that. But here, I think I found it.

Yeah, I can paste this in.

So if you want to look at that. But yeah, so the primary relevance for us will just be, as we're looking at the DNSSEC signing issues, because this goes into the importance of DNSSEC, what it does, and just the stability of the DNS system as a whole, but that would be the part I found to be most applicable to new gTLDs in particular.

And then the, did you have a question Carlos? Sorry. And then the registration abuse policies working group final report. I believe this is from 2010, I would have to go back and look at it again. But I thought this could certainly be used as a source article for us, because even though it's dated, it is an analysis of variations and registration abuse policies, and then this obviously helps inform current requirements, and goes a little bit to what we were talking about earlier with specific types of abuse, formally being forbidden, and that being a requirement.

And so that essentially gives registrars at least the reasoning and the teeth to take down domain names, since they're required to have those explicit categories of abuse listed in their policies. But this, if we do look at anything, even if it's a focus group, or we're looking at something after the fact, after we have more data about DNS abuse, I think this is helpful for just informing the range of abuse policies you can get from registrars.

And then lastly, this last report dealt primarily with bot nets, so it was the SSAC advisory on fast flux hosting and DNS. And you know, essentially as you're, with fast flux hosting, you're dealing with bot nets that are calling out from local machines to domain names that can be changing. So even if you take down one domain name, the software knows that if they can't find the first one to search for the next one.

And so, with that, because you're dealing with bad guys who are using algorithms, to generate domain names, and then buying a bunch of these, or register a bunch of these domain names, and that makes for a highly sophisticated and resilient bot not, but there are, on the other hand, there are known patterns for these types of bot nets. And so it

would be interesting in looking, once we have this abuse data, to know [inaudible] what's hosting more or less prevalent in new gTLDs. And this could relate directly to whether or not a registrar is, or registry is actually taken initiative in their own zone to look for such a thing.

And so those are my readings. Does anybody have any questions? Thanks.

LAUREEN KAPIN: Who would like to go next?

[SPEAKER OFF MICROPHONE]

Brian, microphone.

BRIAN AITCHISON: This is Brian. I have just been confused from a technical standpoint. It's used for phishing attacks, is that correct? Like fast flux phishing is the term I've heard a lot, but they use as a specific technique?

DREW BAGLEY: It can be used in a variety of things, but it can be used, it's especially big with bot nets, you can get that. So, basically, at some point, you would have been phished, most likely. So that you would get the malware installed in your system, and then your system would be calling out to the bot net. But instead of there being one domain name, and that domain name could easily be taking down, what you would have is you could have countless numbers of domain names.

They're generated using the same domain generation algorithm, so that way the software would automatically know where to look next. And the, but the nice part about this is that, you know, there are going to be patterns when you see a group, or an individual or a group of individuals register a bunch of these domain names that are all off by a letter, or a number, or whatever the sequence is, whatever algorithm they're using.

And so that's how they are, there are lots of papers written on mitigation techniques for this, and so this is something where if you had a registry being proactive about looking for these things, perhaps you could see that some zones have fewer than others, or what not.

BRIAN AITCHISON: I think that's interesting, this is Brian again. Some of our conversations with law enforcement building the DNS abuse report, they mentioned these domain generation algorithms that, as something we should focus our research on as a form of abuse. Another interesting tidbit is that we've talked with some professors from the Computer Science Department at the University of California San Diego, what I think is a very interesting study about how this sort of structure and syntax of a domain name is predictive of the amount of abuse you are going to see emerging from that domain name.

So it's something that I'm, I will look into more, because I think it's an important issue. Yeah, thanks.

DREW BAGLEY: Yeah, I would say, yeah, we definitely want to look at DGAs as part of our overall abuse study, for sure.

LAUREEN KAPIN: Okay. So who would like to go next? Carlton will need to step out, so we don't want to break the flow. So David, you're volunteering, yes?

DAVID TAYLOR: I was volunteered, yes. In my areas of expertise as well as even better. So changing poisoning, ICP, so [inaudible] very short after courses [inaudible]. A common practice, as we see there, where we get there, the goal is to make use of the search engine results to draw the good users to the bad sites where the malware is.

That's the main basis of it. And I think the hypothesis I was looking at was whether the new gTLDs were anymore subject to SEP then the legacy TLDs. Possibly because there is a key word, we're getting more key words involved, and this is about key words. So I thought that might well be there, the hypothesis which we need to look at.

I'd put there in the findings, they're trying to get out of that paper [inaudible] probably a lot more needs to be done then just that paper. And how it works, that you've got the hackers [inaudible] to URLs, which are taken from the going to be popular domain names, and then they create a huge number of these URLs containing the targeted key words, which again ties in with some of the new gTLDs, which are key words themselves.

And that goes through, and basically, you know, you've got an intermediary, and off you go. So if you go to Trip Advisor, and you're looking in the comments, and you see that and somebody just pumps in there and says, hey, go to this site, this is really good. This will tell you how to do it, that's where you do it, that's installed, the malware and then you get sort of caught out, shall we say, which those tend to get taken down from the blogs and [inaudible] you can't put them on.

So that was the [inaudible] so that at the end there, there is sort of recommendations. I mean, it was really a setting with the new gTLDs have been targeted more than the old ones, what solutions have been put in place, whether there are solutions in place. I think, X, Y, Z was having a lot of these problems. So again, I don't know whether we, or how we go and found out which ones have the problems and what's being done, but that essentially was where I was going to.

And then the other thing is the search engines themselves, which is just purely for our Google friend, and they're avoiding certain TLDs if they're going to [inaudible] that this is happening, and that's probably going outside of our remit. [Inaudible] certainly take any comments on what the technical people who will know this better than I.

DREW BAGLEY: This is Drew for the record. Yeah, I think this sounds like a great article for us to look at, because I guess there would be the overall question of where new gTLDs are ranking in general in a variety of, I guess, SEO rankings, but if we found that within that universe, there was a high percentage that were bad, and therefore part of this search engine

poisoning, that would be pretty interesting. So that might be something that we want to bring up at the, when we convene at the bigger group when we have our Google expert here, because I know he has access to Google's internal research team, and so perhaps there could be some data for us on that.

DAVID TAYLOR: Thanks. Anything else? Should I move on? Spoofing. And this is where a malicious party basically impersonates another, go about it in a couple of ways. I was looking more at it in the IP and the DNS rather than the RP, but again, here the question here is whether the new gTLDs were more subject to spoofing attacks then legacy TLDs. I think that's the essence, and whether a user can trust a domain name that they're going to, that hasn't had the underlying DNS spoof, and then again, the third one, since the hypothesis, whether or not internet users, can't read it from here, want to be sure when they type in a certain domain name, they can go to the right domain name.

And again, the DNS hasn't been hijacked. So those are the points where there is any difference between the new gTLDs and the old TLDs. And hence there on the right, consider the vulnerability of new gTLDs, and which ones are offering additional protections, if they are offering additional protections, and if they are, to what extent those are successful.

So, again, open to any thoughts, comments on that one.

None? Go on, Fabro.

FABRO STEILBEL: This is Fabro for the record. Just one of the previous ones, [inaudible] use this of the TLDs to best practice. But the question I have is, how I measure it and how we avoid it, because every type of analysis that could be made is after the thing has been done. So, and then for example, in the previous…

I think there is a cross channel.

[SPEAKER OFF MICROPHONE]

The one thing I had in mind here, is that some measurements we do are post-act, and some measurements are pre-act. So all of this, two cases are clear measurement we can have post-act. So for example, one of the papers I review it, they get using the WHOIS information, they get who are the ones that are doing the most damage. And you could clearly find them.

But if you [inaudible] them, it's just, it's probably a fake WHOIS or something like that, it just replace with somebody else, and then would be so hard eventually to get that information, and with new technology, new users, will be so much more used.

It's from beyond.

[SPEAKER OFF MICROPHONE]

That would be one other thing about metrics for that, but the only thing I can see is that looking backwards and say, yeah, that happened, but I

couldn't find a way to kind of use metrics [inaudible]… I'm just sharing your frustration, yeah.

DAVID TAYLOR: Yeah, it's hard to quantify, and if I'm going to the registries that are offering the protection and specifically asking them, which we've got an example in terms of TLD. So I mean again, that's a good example. I'm not sure. So I'll move on to FTLD.

So FTLD, that is registry services for dot bank and dot insurance, and the key thing which they're underlying is their enhanced trust. So they set out and there is quite a bit of paperwork on how they, how this enhanced trust, so I think the hypothesis there was whether the security requirements which they put in place is enough to prevent DNS abuse.

They're different because they're pretty closed TLDs as well. They're not going to be abused in the same way as an open, necessarily an open TLD, the risk is a lot higher with them. My question is, would it be feasible to oblige all registries to ensure a high level of security, where the trust aspect mentioned this morning, the Nielson obviously, I think there is arguments as to whether we should or shouldn't try and put something like that, I would recommend something like that in place, or whether we leave it to the regulated and high risk TLDs.

Going there a little further on the right, I'd put there for, what we could do, study if it's feasible to implement mandatory higher security requirements. And to actually there I was thinking, because with the

GAC, their recommendations, we were talking this morning about their just recommendations haven't been implemented.

And it strikes me that is something we should be going forward potentially as a review team, saying that, this has been a clear success if we can identify that's been a success and isn't this something that should be mandatory rather than a recommendation? Because I found it quite confusing when you speak to people as to who thinks it's a trusted TLD, because you're not dot com, and then you go, well, it isn't really.

It means nothing. And I think that's, for me, it's an issue. And maybe we can get some impact or some response from registries as to those who have put in higher security or practices that they're saying this is far better, and this is the benefit on high registrations, etc. So I put there identifying with other new gTLD registries that have been put in place, enhanced security.

The only other one I really know about is dot trust, and that's appropriately named. And I put there as well, which is just throwing into the wind, tangibility of a position of prohibiting proxy privacy registration services. Just like to throw that one out, because it's one of those things which is an interesting one to debate, shall we say.

And that's what considered the recommendations, the WHOIS review team, because we certainly wouldn't want to be going down and redoing there, their work, shall we say. So any comments, thoughts on that?

UNKNOWN SPEAKER: Yeah, maybe what we can do, because I found a way to kind of like, higher security requirements, but then for dot bank, for example, we [inaudible] bank [inaudible], but we have ecosystem that would be really hard to define a question to what is bank or not, in all of the world. Although, I review the [syntax?] report, and they kind of ones, at the most use it for fraud. And with the Nielson research, we also know that those are the ones that are most trusted.

The user report [CROSSTALK]…

DAVID TAYLOR: …the Symetech dot bank is the most abused.

UNKNOWN SPEAKER: Yeah. The financial ones are the most targeted for it to use.

UNKNOWN SPEAKER: Most targeted, but not necessarily… I don't know if there is like a conversion rate.

UNKNOWN SPEAKER: Targeted, yeah. So what we could suggest is a greater group of five, so those who for reasons A, B, C, are highly used it for attempts for fraud or something like that, they will be review it for implementation or implementation or metrics. So we don't discuss the criteria itself, because it would be crazy for all gTLDs, but they have a small group of

ones who that are very highly visible for fraud, that would monitor them.

DAVID TAYLOR: That also opens up into other TLDs as if there is, we can identify TLDs that are abused, or attempted to be abused, that if we arrive at a certain threshold, then more security needs to be put in place, for instance. That might be something which I don't think is generally discussed, but it's not which we could possibly suggest.

UNKNOWN SPEAKER: And I'll be naïve in a way of what I am going to suggest, but we could ask private sector about for inputs and which one is the most tempt to fraud. I mean, not sure if it will work, but we could find ways to… The thing is, how we set the criteria to what are the top use it for mistrust, or abuse, or…

DAVID TAYLOR; I'll carry on. So then the other one I've got was the name collision occurrence management framework for registries. So I wasn't sure about this one, coming in, but it's worth TLDs being used on an internal network, so that if you find a query for that internal network, it could go out to the public DNS. I know that was a big thing when that came up after launch and this is 90 day period put in place, and I can put this, and this is quite an old document, I think it was 2010, so it was sent in the early days there.

So the hypothesis really was, did this framework work? Were there examples which show that collisions were avoided? And there was a terminology of whether there was an emergency situation if that occurred, then certain things would be done. Now, I'm not sure there isn't, somebody could probably tell me, there is a report on the effectiveness on this somewhere, seems that was 2010, but maybe there isn't.

If there is, then we might have our answers, and that's fine, we could review the effectiveness, then I'm not quite sure what we do, or how we go next. So, there the recommendation, whether we've identified as any ICANN or registry reports on the effectiveness of this, and then whether things could be improved in the future.

So open to any comments on that.

DREW BAGLEY: This is Drew for the record. I can't recall now, but how long ago it was, wasn't it two months ago? We had a presentation that addressed this specific issue. And so there was recent data on it, and wasn't it one of these things where there is, there are…? We've seen no issues for it, and so therefore we don't know if it was the success of a safeguard, or if it's because it wasn't the big issue we thought it was.

I think this is where we were having a discussion that it was like the Y2K bug, so maybe you guys remember which month that was. But yeah.

BRIAN AITCHISON: This is Brian. That was a presentation from Francisco Arias, and I believe there are, there is name collision reporting out there, that he would have access to. So we could, I can make a note to follow-up on that. I feel like he's told me about… Karen, do you remember that?

KAREN LENTZ: No, I was looking for that too. I don't recall when it was, but I, from what I recall, from what he said was the number of reports is somewhere around 20 to 30, and that none of them had been threatening, or whatever the right terminology was. But, you know, maybe we can go back and point you to that recording, because I do recall pretty interesting discussion about the sort of preventive effect, which was [inaudible] in other sort of perspective on this set of risk and the measures that are in place.

DAVID TAYLOR: And the other one is [inaudible] which I didn't get to, there is the high security zone, top level domain advocacy group, which I started working through that was 48 pages, and I got through to about halfway through, and this was on the flight where sleep took over. I'm not saying that was boring, but it was clearly, should we say, there was no consensus, but there was different positions.

So you had to dig down, and there is some quite interesting stuff at the end as well, so I jumped to the end where you've got a lot of the various entities are put in public comment and seeing where that was going, so that was something which I realized I wasn't going to get through in half an hour.

And the other one, which is up there for me, measuring perpetrators [inaudible] squatting, which is an article by Ben [inaudible], who is very good. It was something I actually wanted to read, and so there was a part of me that thought I would get up this morning and read that, but then the other part of me thought no.

But I do actually want to read that one. That's the one that actually hits on my competence level, I suppose, so I will read that one and get back to you on that.

LAUREEN KAPIN: Okay, so it's 3:40, and I don't want to have us launch into the next presenter. So in the interest of recapping, maybe I'll ask both Drew and David just to give a yea or a nay as to whether the articles they have presented on should be a primary source, a primary source for us or not, because I think that this is useful. And also Alice, I think that goes to our, that other category of useful, non-useful.

And I just wanted to make sure we capture that as we go along. So if it's just going to be… If the article is just useful as background, or you know, explanation, but isn't going to be useful as sort of a primary source for our review team, if you could just indicate that. That way we can keep up an ongoing tally of what our smaller subset of sources are going to be.

This is kind of a universe so to speak, but we're going to be narrowing down to a much smaller solar system here. So Drew, why don't you start and then David, you can tag along. And then we'll be ready for our break.

DREW BAGLEY: Alice, would you like us to just highlight these green organizationally? So that way you know what we would like to use as a primary or keep as a primary?

LAUREEN KAPIN: Yeah, that's fine, that's fine. Yeah [CROSSTALK], yeah, that's fine. So in the Google Doc, if folks can use the red light/green light convention, if it's going to be a primary source, use a green color for the title of the article, and I'll say just do it that way. That way we don't have to do red. So if it's going to be used, just designate it in some green font. Does that make sense? Yeah? Yeah?

Okay good. It's 3:43, I bestow those extra two minutes upon everyone for the break. And we'll come back here, we're going to come back to the other room, so Alice, tell us where we're going to be.

ALICE JANSEN: Yes, the next meeting is in the forum room, which is just down this hallway and to your left. Just, you'll see it.

LAUREEN KAPIN: So it's forum. Just us.

[SPEAKER OFF MICROPHONE]

I designate you as my negotiator here, David.

[SPEAKER OFF MICROPHONE]

So gather what you're going to need, and we'll meet back in the forum room at 4:00.

ALICE JANSEN: We'll be back in this room to conclude the day.

LAUREEN KAPIN: Yeah, that will be at 5:00. Okay?

[END OF TRANSCRIPTION]