SAN JUAN – GAC: PSWG Meeting
Tuesday, March 13, 2018 – 08:30 to 09:30 AST
ICANN61 | San Juan, Puerto Rico

CATHRIN BAUER BULST: All right. Good morning everyone. And thank you very much for joining us here in this large hall instead of staying outside in the Caribbean sunshine after the wonderful gala yesterday evening. We appreciate your dedication to the Public Safety Working Group so this is the official meeting of the governmental advisory committee Public Safety Working Group. My name is Cathrin Bauer Bulst. I'm one of the now again 2 co chairs of this working group and here with my co chair Laureen Kapin. Now we have 2 main points on the agenda and we will be talking about the Public Safety Working Group's work plan and then the work of OCTO and the DAAR tool and we are going to start off with the Work Plan but first I will give the rest of the Public Safety Working Group people a chance to say good morning to you as well.

UNIDENTIFIED SPEAKER: Good morning folks, I'm Laureen Kapin with the United States Federal Trade Commission, focussing on consumer protection and appreciative of folks joining us for the first session and although we have from 8:30 you will from wait there's more.

After this session we are actually going to be switching topics and focussing on the who is system, and the GDPR so you get a big dose of us this morning, and hopefully it will be, hopefully it will be at least pleasant tasting and interesting.

IRANGA KAHANGAMA: Hi, good morning. Iranga Kahangama with the U.S. Federal Bureau of Investigation. I wanted to say thanks again for attending. In terms of topic I'm working on the DND abuse issues which relates to DAAR where we have some of the OCTO folks and I welcome you to look at the slides and think about ways we can support either through policy or other recommendations we can support the initiative. It would be beneficial for the security of the Internet community. I look forward to chatting with you through the Work Plan. Thanks.

CATHRIN BAUER BULST: Thank you very much. So we are going to launch oh, yeah. Actually that would be. So Laureen just made a good suggestion which is to for those of you who are members of the public safety working group to just stick up your hands so that people because we have a lot of people in the audience to have an interest in our work and who might be interested in chatting to one of us also as the day continues. So could I ask the members

of the Public Safety Working Group just briefly stick up their hands so everybody can see where they are.

LAUREEN KAPIN: These are the folks, if you have questions it's not just us on stage. We have lots of members. And they are all happy to chat and answer questions.

CATHRIN BAUER BULST: You know from Sunday's session we are about to adopt the Public Safety Working Group Work Plan for the upcoming time period. We've been over at a high level on Sunday, and we want to take a chance now the opportunity now to walk you through it just once more and see whether there are any final comments on this before it gets adopted in the GAC communique at the end of this meeting. The first goal surround around abuse litigation and Iranga is the topic lead and will walk us through.

IRANGA KAHANGAMA: Thanks. So like I mentioned before this is one of our main work plans, and it's the goal is to put ICANN in a better position to address DNS abuse. There are a number of communities that identified this as a high priority. There are a number of reports the teams have put in and we want to continue momentum many. To ... as I mentioned the domain abuse activity reporting

project which you will hear later is a big Work Plan item for us. And then for those interested there's also the GDID marketplace and the identifier technology health index, 2 separate programs surrounding ICANN's open data initiative which is attempting to put more data, more numbers behind some of the abuse since some of the health at a macro and micro level so we are in a better position to report on that abuse so skipping down a couple of bullets I think all of that to say you can leave it we are driving that towards creating principles. Generic kind of base line understanding mechanisms we think should be mutually accepted by all parts of the community and we can agree upon and commit once we agree upon them as a group. And then in terms of new work I think one other community we haven't tapped into fully yet is the SSAC and we have heard they are doing a number of initiatives that are interesting and we would like to engage more formally with them. So I think for this meeting there is a session 3:15 pm tomorrow which is the SSAC open meeting which they've mentioned any one and everybody is open to come and may be interesting to attend that and see some of the security items they are working on. They are interested in registration services and the technical aspects behind that which is obviously interesting given some of the GDPR considerations. And so I think there are a number of security oriented folks on there so in terms of outreach we are going to try to more formally establish a relationship with them

so that we have a better feedback mechanism. So that's kind of the main overview of what we are trying to achieve there. I welcome any one who has ideas. We are obviously open. There are lots of security issues with the Internet, and the DNS so we have limited band width but I think we are doing well and we will be sure to update you as items kind of break. I think for this meeting it's been a little bit a back burner just because the GDPR issues has take a lot of our attention but it's something we are to going to keep on as high priority. Thanks.

CATHRIN BAUER BULST: So let me remind the GAC members among you that you also have a copy of this Work Plan as annexed to your briefing for agenda item 11 because we introduced it to you again on Sunday so just in case you want to scroll through at your own pace and leisure that's where you can find it.

LAUREEN KAPIN: So briefly on consumer safeguards this is actually been an issue that the consumer trust, consumer choice and competition review team has focussed on in part, and I have led the subteam focussing in on safeguards, but basically this topic is a continuation of our existing work which is to advocate for policies that protect the public on line. That's sort of the top level goal of this part of the Work Plan so we participate in

relevant reviews. We liase with various parts of the ICANN organization particularly compliance and security, and also we liaise with the community to talk about the issues because everyone has a vested interest in keeping the on line environment safer for users and inspiring consumer trust so that they continue to use the Internet. So in that regard there are lots of different stakeholders and WorkStreams, and that includes the new subsequent procedures review PDP rather, and we are also assisting with implementing the privacy proxy services accreditation system, so lots of different work streams that are going to continue in that regard.

CATHRIN BAUER BULST: All right. I will take the next 2 points on the subsequent page on accountability and on preventing exploitation of the DNS so on accountability we are actually still looking for a topic lead to take charge of that point. And that's an ongoing topic for the Public Safety Working Group. There are a number of work streams related to public safety that are of relevance to the policy side to be more effective in preventing some of them and that work has included where there might be an expectation on behalf of the users that that is a safe space for children, and the safeguards that have been done the Beijing communique need to be evaluated in terms of effectiveness with a view to possibly adapting them in any subsequent detail rounds and there are

some other work going on in the WorkStream. I won't go into in more detail here but please come talk to me or the Italian GAC team about these efforts. I will stop here and see if anybody has any comments on the strategic goal one. Let's move to the second strategic goal which focuses on the RDS in particular and one major item on that is the who is and the access to the GDPR registration data so Laureen.

LAUREEN KAPIN: I am going to park that as we say because we are going to be discussing the topic in depth right after the coffee break so this is just to know for you that the WHOIS system and all the benefits and responsibilities that go with it are part of our WorkStream and indeed that's been a real focus of our more recent work.

CATHRIN BAUER BULST: That brings us to the next generation RDS PDP. Greg do you want to say 2 words about that? No. Okay. So I think.

UNIDENTIFIED SPEAKER: Ongoing.

CATHRIN BAUER BULST: Ongoing, yes. Then we have the registration data accuracy efforts which as you know has been on going for a long time, there is now some implementation of checking of accurate syntax of registration data entries. What the community has not yet tackled is the actual checking of the identity of the registrant, and theres still a lot of room from a public safety perspective to an increase in the quality of GDPR registration data and we see some promising initiatives also in the ccTLD world how this can be accomplished in a reliable get not too costly fashion, and I think we will continue our efforts to look at how those efforts could possibly scale and translate also in the gTLD world.

IRANGA KAHANGAMA: I think this is an important Work Plan section and because there is what most people don't forget about is GDPR calls for data accuracy as well as part of the responsible need to have data, so I think this has been something we haven't focussed on because right now we are just trying to keep the data or maintain access but we haven't hit that second step of making sure that data is actually accurate, and so I think as we go forward is ... that's the performance in relation to the is the key tool is the RDS review team where the GAC nominated from the U.S. Lily ... from Interpol and myself to participate. That review is currently on going and still in the early stages, and we will report back to you

on its efforts probably at the next ICANN meeting in Panama. So one more reason to come to the next one.

LAUREEN KAPIN: That is our strategic goal 2 bucket. Does any one have any questions or comments on that? Okay. Then we are going to move onto strategic goal 3 this is kind of the foundation. The bones strategic goal. Build defective and resilient PSWG operations so this really focuses on our organizational framework, and our procedures. So you will see that developing a Work Plan is the first thing. Strengthen leadership. Make sure as we had mentioned on Sunday we want to have a deep bench so that we have people to be able to focus on the many important topics that take place in policy development efforts and stakeholder outreach. We want to strengthen membership this. Falls into the pledge drive category. One of the ideas actually that we had discussed with GAC leadership is encouraging member of the GAC to consider nominating and really reaching out to the law enforcement and to... every country has law enforcement folks and people arrest knowledgeable about about front line investigations and how you deter criminal activity. Particularly as the DNS is involved and we know that these issues get technical and complicated, and you have experts within your country that you can consult with and we would encourage you to do that formally, and reach

out to those people, and better yet, nominate them as an advisor to the Public Safety Working Group. Have them join our e mail list. Come to the meetings if they are the resources for that. So this is a really important point about how we really get everyone very involved in these very important issues of public safety, so I did want to highlight that, and then of course we are an advisory committee to the governmental working group of the governmental advisory committee so we want to make sure that we are communicating consistently with the GAC and with the GAC leadership, so you know working on and giving you a heads up when there are hot topics that require quick action and we've had a great illustration of that recently where we know we've been asking you to look at things that are complicated and review it quickly, and that's not the ideal situation, but unfortunately, that's the situation we are in, and we want to make sure that we are doing things as effectively as we can to give you a heads up and to give you an opportunity to review important work by the PSWG, so we can get your input and endorsement and we can work with you to make sure that the product reflects consensus GAC position so that's in our Work Plan to too, and in that regard we are always very mindful of of wanting to hear from you what we are doing well, and what we can be doing better. So please don't be shy. As you can see, we are not especially shy, and we are happy to talk with you in the hallway, on the telephone. Any time if you think there are

adjustments that need to be made. So that is strategic goal 3 of our Work Plan and I'm happy to invite questions or comments on that. The Jays on.

CANADA: I am a Jason, a member of the public safety group from Canada. It was noted in Abu Dhabi about the fact that we are a relatively mixed group a lot in North America and a lot from Europe and we would like to diversify our membership and if you have people that you think would be applicable candidates to work with the public safety working group please approach us and we can tell you how to get involved. The more diverse we are the stronger weary think is probably the message we would like to send out, and that the fact that a number of us are from North America or western Europe, we would like to get viewpoints from across the world and not just our respective states, so please approach one of us, and we can certainly help you get involved or help someone from your police force get involved with public safety. Thank you.

CATHRIN BAUER BULST: Thank you so much, Jason for making this very important point. This is Cathrin. And I just want to add the more diverse we are. The better we reflect the full GAC so that's something that is of great importance to us as we work, as your working group to

help do you your work and we can do that better if we reflect the various positions on the GAC also in the working group. And just to say that a lot of our work actually does not take place at these meetings. We have monthly phone calls among the full working group. We are weekly phone calls among the leads and the membership and doesn't matter where you dial in from. It's the usual Adobe room. If you want to nomination Naya expert who will not be able to attend that's key. It's better if you can meet people face to face once in a while but most of the work that we do on substance takes place outside of the meetings through remote participation so I wanted to encourage all of you who are worried for resource reasons about investing in the work of the Public Safety Working Group that should not prevent you participating. So I will just stop here and see whether there's in any further comments on point 3? Or if anybody is so enthusiastic they want to jump up now and join.

[Laughter]

Just kidding. If there's no other no further comments we will move to strategic goal 4 about outreach to other parts of the community and to stakeholders outside of this environment. So it's well and about assessing what we are doing in our Work Plan. So one key point is to ensure that, that insetting our priorities we are setting the right priorities, and, of course, for this we need to talk to those of you in if the room but also to a

number of people outside the room and figure out what is affecting them in terms of the policy that is being made here, how implementation of the current policy is working for them, and where there are opportunities for improvement or even big problems that arise that they would wish the public safety working group to in inform the GAC about or to provide expert input on. We are also working to develop awareness of the Public Safety Working Group by other government agencies to make sure there was horizontal coordination and countries are aware of the ability to provide in ...to the Public Safety Working Group because of course this is not just about police. There is a lot of public safety issues that the Public Safety Working Group is officially in charge of that need to be fully reflected in our work. And then again we are working on lowering barriers to participation. Also by means of providing better information. I mean you probably are all familiar with this by the time I have explained to somebody what happens at ICANN, people are either fast asleep or you know the hour that I have for my meeting is up.

[Laughter]

So it's really challenging to get the right kind of input because when people come back and they're like so what did you decide at this meeting? What are we doing on this one? Actually we just sort of talked and things are moving but it's taking a while.

Of so for many reasons it's very difficult or it can be very difficult to get people to be both sufficiently apprised of what happens here and why it matters and then to put them in a position they can identify why it is important to them, and what they can contribute. And we are working on ways to basically lower those barriers. By means of newsletters. Are short summaries of what happens here, of trying to make our work for accessible, to those who are not dealing with Internet governance issues on a daily basis, and we had some very good inputs during our inter sessional meeting in particular on those points because there we had a lot of agency that is don't normally participation in this work and who asked a lot of very good questions about why we do certain things and how we do them and who had good ideas about what we do to do better reach out that them so we're working on implementing those ideas. And as you can see here there's also more room for volunteers to come and join our effort. I feel a bit like fundraising.

[Laughter]

So…

LAUREEN KAPIN: And Iranga will talk about outreach efforts we had during this meeting.

IRANGA KAHANGAMA: Thanks, yeah, so this might and appropriate place to just briefly mention again we wanted to try and start talking to the SSAC. They mentioned they are exploring interesting things and in the course of outreach we've chatted with registries and registrars about some of the RDS issues with who is just trying to get their input on feedback on how they see all this going. So those have been the 2 kind of main outreach external things we've done. OCTO obviously we are going to start talking to them in a few minutes we are when we talk about DAAR and we are open and I think there's a lot of creativity in this so if you think anybody has other crea ... we would love to explore that.

CATHRIN BAUER BULST: Thank you, and in terms of getting to know our parts of the community better I want to remind everyone with about the social event with the registrars this evening. I think it's starts at 6:30 on the terrace. So please join us there. If you also want to participate in getting to know other parts of the community better. And I think that is concludes well I will stop for a minute and see whether there's other creative ideas on point 4? And if not so that will conclude our review of the work plans. If you have any other other comments or questions or suggestions or changes to the Work Plan I would ask you to either approach

one of us or send us an e mail by the end of day today and otherwise we will consider this point closed and we will propose language for the GAC communique to adopt this Work Plan. All right. So we are all set on this? And that means we can move onto our second point of the meeting which is the conversation with OCTO and DAAR if oh great I see David walking up. David thank you so much for taking the time and doing this despite what I understand is a serious cold.

DAVID CONRAD: Good morning, apologies for the hoarse voice and I may cough once or twice but I'm filling in for John who appears to have had a really good time at the gala last night.

[Laughter]

And this is not a result of the gala thank you. Moving on to next slide please. So I'm sure most of you here are familiar with what DAAR is for those of you who are not aware DAAR is a reporting system we are developing with the help of the iThreat cyber group to track abuse that we see interested in with the ones identified by the GAC in the Beijing communique. MODULO which isn't something that we can see in our vantage point at ICANN. As well as SPAM. How does DAAR differ from the myriad of other reporting tools out there? Basically it is the way it differs via the amount of data that we collect. We have basically

aggregated a whole bunch of feeds. The term of which the data is collected we actually plan on keeping data to allow for historical studies. And focuses on a multiplicity of abuses, so that we can generate information that is transparent and reproducible to facilitate communication, to facilitate policy development within the ICANN communities. Next slide please. I've already spoke about this. So the one issue here is that we license a good portion of the data that we are using for DAAR and that data may or may not be available. Next slide. So what can DAAR be used for? So obviously it's primary goal is to report on the threat activity at a top level domain or registrar level. It can be used to study the history of a security threats or domain name registration activity. It can help the operator the registries and registrars and back end operators understand or consider how to manage their reputation in the anti abuse systems. The reputation lists and those sorts of things. It allows us to study malicious registration behaviors, and it is aimed at helping to assist the security the operational security communities. We use TLD zoning it collects all of the data for the gTLD registry analytics. It's mostly using the centralized zone data service, and where possible we do zone transfers. DAAR will only use names that appear in the zones. We don't try to look into the registry or registrar databases prior to those names being dumped out into zones currently we have about 1240 gTLDs which works out to about 195 million domains. We have been

approached by a number of ccTLDs who wish to participate in DAAR and working on incorporating them into the DAAR system DAAR also uses WHOIS. We use a small part of it. Primarily the registrar but even that turns out to be quite problematic. The since DAAR is focussed on trying to develop a system that is reproducible by any one we are not using any information that is available internally within ICANN, and only within ICANN. We are actually using information that's available to the public one way or another. As a result of this, you know, we are trying to extract information from, for millions of domains through the existing WHOIS servers and as many of you know rate limiting can be a bit of a challenge. Next slide please looking at the threat data sets we use quite a few of those. We do try to unique FI the data so that we don't have false as many false positives. We use multiple domain or URL abuse data sets generating daily counts of domains associated with phishing bottom of the Internet and SPAM. We calculate photo ASL and cumulative abuse domains and create histograms charts and days in the life use the focus of DAAR is to reflect how people outside of ICANN and the ICANN community see the domain name ecosystem. Next slide. Next slide. We within OCTO or ICANN don't compose our own block list. That's not our job. And I doubt we would be able to do it well. We present a come posit or aggregate of the data available through external parties that are those parties generate those lists to actually block threats. DAAR collects the

same abuse data reported to the industry so we are not generating anything new here, one of the common concerns that people have is that we are generating new data that may not be accurate, and we reiterate the point on multiple occasions that this is what Internet service providers, mail operators all use in day to day operation. We are not doing anything new here. Next slide. The criteria for inclusion of one of these representation block lists into the DAAR system. They have to provide a threat classification that matches the set of threats that we are looking at, the operational security communities must trust that RBL for accuracy and clarity of process. They have to have a positive representation in the academic literature, and the RBL has to be broadly adopted and accepted across the operational security communities and that's demonstrated usually through the fact that the feeds are incorporated into commercial security activities, and products, they are used by network operators to protect their users and devices, and they are protected by or they are used by e mail providers to protect to prevent SPAM and other attacks the next slide. The RBL as we use are ubiquitous. They tend to block more than just unsolicited commercial e mail. They are used in browsers for example Google chrome uses the APWG list. They are used in cloud and content serving system ... uses SERBL and Amazon as Web I forgotten what WAF stands for uses RBL to block abuse in volumetric attacks and Google safe blocks

malicious URL and ad word fraud. RBL are used in the DNS through something called resource policy zones, visually developed but is now being used in multiple resolvers and SPAM how is and others provide these RBL's using the RPZ format relating more of how the resolvers are used this is so we are not going out on a limb here and using stuff that's experimental. It's stuff that's actually used in production services as well as commercial products. Next slide. We also have been looking at academia to review these RPL's to ensure your that they are using best practices and are used in ways that researchers can trust, and that's a list of a number of academic reports that are making use of the RBL's we use within DAAR. Next slide. So the current set of RBL's we use are the SERBL domain only list. SPAM house domain block list. The anti phishing working list. The malware patrol which is a composite list of all those you see and the right, phish tank ransomware tracker and THEODO tracker. Next slides DAAR does not identify all abuse. There is no reputation provider that can see all of the abuse. Each has their own view of the Internet abuse, and the different RBL's are focussed on specific things. So we have one of the reasons we do the aggregation of these RBL's is to try to get more of a composite view of the Internet. Next slide. We frequently get the question, why we are reporting on the on the SPAM domains. So in the HIDURABOD communique there was an expression of interest by the GAC for information related to SPAM. And from

our perspective most SPAM is sent via illegal or duplicitous means, that is typically BOT nets. Of it's no longer singularly associated with content via e mail, there is link SPAM. There's tweets SPAM. There's SPAM within like Facebook, and other messaging systems. SPAM is actually the primary means of delivery for most of the other security threats. The ones that the GAC mentioned in this their communique from Beijing. You could sort of see SPAM as a cloud service, the avalanche BOT net provided domain name registration to customers in order to actually facilitate the transmission of SPAM what. We in DAAR use is the domain names found within the bodies of the SPAM message. That is the things that people will click on in order to you know trigger a malware download or that sort of thing. Sort of most importantly, the SPAM domain representation influences how extensively or aggressively security or email administrators apply filtering. You will generally find that the system administrators focus first on SPAM because it is a very good indicator of compromised domains. Next slide please. Next slide. So right now the DAAR system is in production. We have been using it internally for some time. We have not started publishing the reports that DAAR generates because we want to do things right as opposed to quickly, so what we've actually instituted is a external third party independent review of the methodology that we are using for DAAR to collect data. And those reviews actually one just finished like yesterday. The

second one is due in a couple of days. We are going to simply pass those reports through to the community, if the reports provided any suggestions of change, we will of course make those changes. Our intent is to take those reviews and provide them to SSAC and ask for SSAC's input what we should do with the methodology DAAR uses but at this stage the internal reports and the graphs that you will see, are currently internal only. They should be available our goal at this stage is to start making this stuff available to the community for discussions related to policy about the DNS abuse before Panama. So in this slide you can see the all the gTLDs that have at least one reported abuse domain over time and it shows you know the different colors show how those reports of abuse vary over time. Obviously SPAM is by far the leader in terms of reports, but we do see phishing, malware and BOT nets. Within the DAAR system or the within OCTO one of the things we've done is take the data generated by DAAR and do these bubble charts. If we had animation you would see these things growing and shrinking over time. That's actually makes for sort of an interesting you know LAVA lamp of display if you're Board. This shows the phishing domains abuse and in general the larger domains are it's all sort of within a relatively narrow band. Next slide. You do start to see some out liars. Things that are going sort of out of the realm of you know the statistical normal, and our intent in the future is that we will be publishing the names that actually

give people an idea of which of the registries and registrars are being subjected to more abuse than others. Clearly SPAM gets a whole lot more interesting and particularly when you vary this over time. These bubbles go up, go down. Left and right, so it actually is a very interesting display providing some interesting information relating to what's called flocking of abuse from multiple from one registry to another over time. Next slide. So this is looking at the per cent of the resolving domains in legacy versus new gTLDs. As you can see the legacy is still you know sort of out numbers the new gTLDs both in terms of SPAM or in terms of abuse as well as in terms of total registrations. Next slide please. Per cent of abuse of domain. Per cent of abuse of domains listed in DAAR. Again this is showing sort of an increase for legacy over time with a decrease of in the new gTLDs. One of the things about DAAR is for someone who's interested in abuse, it provides an amazing amount of data to just sit there and go what the heck is going on? Which keeps my team pretty entertained probably for the best. You don't want these people out on the streets at night! Next slide. Where is the abuse concentrated? So here, these statistics show that the there's relatively a small number of domains that contribute the sort of the vast majority of abuse. This is something that's been known you know sort of anecdotally for some time. DAAR is providing us with concrete data that actually shows this. In ex slide. Project status. Next slide. As I mentioned our focus is on doing

is right as opposed to doing it fast. We as I mentioned we have the reviewers reports are coming in, we are tuning the collection system, the RBL's that we use fairly consistently to ensure timely and resilient updates. Version 2 is under development. There's we are hoping to automate a lot of the reporting so that we minimize the amount of manual labor involved to ensure that things come out in a timely fashion. We are looking at granular attribution, and we are experimenting with some additional measurements. Next slide. Good that was it. The one area that we are sort of finding the most challenging with regards to DAAR is in the context of collecting information about the registrars much that's a function of the who is, rate limiting, and right now we are unsure whether we don't have sufficient confidence with the registrar related data to feel confident in publishing it in the first release. We are hoping that in later versions it does require some thought about exactly how we can collect the registrar data, in an effective fashion. And with that I guess I will throw it back to Fabien or if there are any questions I will be happy to try to answer them.

CATHRIN BAUER BULST: Thanks Dave for that great presentation and I just want to tell you how appreciative we are that ICANN is engaging in this effort. And I think going to be crucial for policy development efforts because it's going to put under the microscope what

problems are worthy of attention in our policy development, and where where perhaps procedures need to be changed or improved to combat certain types of systemic and abuse that continues unabated. I thought it would be interesting to hear what needs to happen, do you think, before this initiative will be in a position actually to publish information about where the abuse is in terms of specific domain, registries. Registrars, etcetera?

DAVID CONRAD: As I mentioned the focus we are taking prior to publishing the names associated with the data that we're seeing is to get external independent third party review to verify that you no he we're not doing anything silly or stupid with the data, to minimize the chances that there will be false reports that people will get misattributed as being a source of DNS abuse, and to try to provide a level of confidence to the community that the data that we are providing is useable for you know sort of concrete data driven information for policy development. We are, as I mentioned, one of the independent reviewers has finished their work. The second one should be done within hopefully within a couple of weeks, and then once that is done we will make those reports available, and then begin the process of associating generating the reports to publish to the community that indicate

you know, where you know what the statistics actually are, and who the actors within those statistics.

CATHRIN BAUER BULST: And you mentioned the term rate limiting and I'm not sure everyone understood what that means and I was hoping you could give us a brief explanation.

DAVID CONRAD: Sure. So any sort of network service can be subject to a DANAL or service attack by initiating a connection more quickly than that system can cope with it so it's fairly common practice for network operators and service operators to impose a limitation to cut down on the number of connections that can occur primarily to stem abuse. In the context of the registries and registrars a number of, in fact, as far as I know all registries and registrars imposed rate limit to try to reduce people sort of scavenging through the database to obtain contact information that would be used to generate SPAM and other attack vectors. So the side effect of that though is for researchers who a trying to collect information to attribute the registrar the domain names to registrars it means that we have to deal with those rate limits and you know in some cases, you know these rate limits are fairly extreme like you can only submit like 5 queries an hour or something like that. The rationale for providing the

rate limits are you know entirely reasonable, and you know prudent mechanism for network operations, it is it would be nice if we could figure out some way that accredited or acknowledged researchers could be white listed so they wouldn't get rate limited, but that is something that we are still sort of struggling with at this time.

CATHRIN BAUER BULST: Thank you so much Dave, and just to this is Cathrin for the record. And just to emphasize the point on the accountability of individual actors. I understand there have been one specific complaint about a specific registrar which in your diplomatic terms, suffers from or is subject to disproportionately large amount of abuse, and I understand one of the concerns about the complaint is that it is based on the SADAG report whose days a stems from are January 2017. So it's not relying on the most up to date data and I think that's one place the DAAR report will be of value because it supports an ongoing and continuous analysis of abuse as it develops in relation to specific actors and will enable these sorts of a kind of transparency that will eventually also hopefully support compliance efforts so we very much appreciate the work you're doing and this, and we are running up against the clock but I just want to see whether anybody wants to ask any final questions before we close this session?

LAUREEN KAPIN: I have one last question I think will be a good sequeway, and that is of course you are aware of potential changes to the WHOIS system and I'm wondering how that's going to how you think that might affect the DAAR initiative.

DAVID CONRAD: So fortunately the DAAR system does not make use of personal identifying information. The only information that DAAR for our purposes with ICANN makes sues of at least relevant to the reports that we are talking about generating is the registrar information associated with the domain name. All the other information is useful when you're actually trying to drill down and trying to understand you know a particular attack vector or something like that but for the purposes of generating the report, the registrar information is the only information that we actually care that much about. In theory. At least, that information should be available via the public WHOIS, you know without requiring gated access, but you know, as everyone knows that there are on going discussions and the final decision on you know what information is made publicly available is still as far as I know still up in it the air.

LAUREEN KAPIN: So this will... efforts of the initiative. It's going to benefit the community and I also know it's a lot of work so we appreciate that. So this is going to close out part one of this PSWG discussion which comprised our Work Plan and then zooming in in on particular initiative by ICANN that's going to help shine a light on where DNS abuse is occurring and inform the community about trend, so it can fuel policy development, so we are closing out this topic, and voila boom presto now we are moving on to the second topic. Which is on WHOIS and the GDPR. So I will turn it over to our GAC leadership.

[END OF TRANSCRIPTION]