MONTREAL – GNSO - RySG Membership meeting 2 of 2
Tuesday, November 5, 2019 – 10:30 to 12:00 EDT
ICANN66 | Montréal, Canada

DONNA AUSTIN: Okay. One minute, folks, and we'll get started.

UNIDENTIFIED MALE: It is Tuesday, November 5th, 2019, at ICANN66 in Montréal. This is the GNSO RySG membership meeting, two of two, at 10:30 in hall 511c.

DONNA AUSTIN: Okay. We're going to take some time to talk about DNS abuse. I have a vague idea in my head about how we're going to do this but it's not perfect. One of the reasons for that is because there has been some information coming through. I think it was on Sunday or Monday that we saw the BCs come out with a statement on DNS abuse. I happened to come across recommendations from the Security, Stability, and Resiliency Review yesterday and there are some recommendations in there on abuse.

I guess what I wanted to talk about … We have the open letter that we wrote and posted to the community on the 19th of August. But amongst ourselves, we've been talking about DNS abuse for a while because we were talking about it primarily in the context of the compliance audit. I think we came through that pretty well but now the focus from the community is largely on contracted parties to try to respond to this abuse problem.

One of the challenges we have is that DNS abuse means different things to different people so the scope is either really narrow or really broad. But my sense is that where the community is headed is regardless of how you define it they want to see something in the registry agreement or registrar agreement to solve the problem. In my mind, we still don't know what the problem is because ICANN has not articulated that. I don't think they're going to articulate that. I think they're waiting for us to decide what the problem is and find the solution.

I guess the conversation I wanted to have today is, I'm assuming that what we don't want to happen as a result of this conversation with the community is more regulation that is reflected in our contract. We're an industry that's supposed to be self-regulating so it's on us, I think, to show that we are actively responding to abuse. Perhaps we're doing stuff to mitigate abuse before it starts but I don't think as a group we're particularly good at sharing with the community what it is we do.

We've stepped up a little bit in that regard with the open letter. Brian's pre-webinar that he did was pretty clear in outlining what the responsibilities are within the registry agreement. I guess I'm interested to understand from this group what we want to get out of this discussion this week. I know we have a plenary session that Brian and Jonathan have been involved in the development of. We have the PSWG coming in at 11:15. I want to understand from this group, what is it that we want to get out of this discussion? And what's the best way for us to get there?

Jonathan talked with a few of us earlier this week. “What are the key messages that we want to take forward?” Now, we’re already into Tuesday so we’ve only got two days left of this week. But what are our key messages? What’s our posture? And how are we going to achieve what we want to get out of this discussion? I’ve got Maxim and then Ken. Maxim?

MAXIM ALZOBA: Actually, I think we shouldn’t be the only ones who are a bit critical of those suggestions. If the suggestion of the BC is read well it has, for example, the issue of impersonation. To resolve that issue you have to have power to summon someone with the password to the office. Most probably, At-Large is not going to be happy about that. To say more, they are suggesting quite serious things to be done on behalf of the tool which is, I’d say, not so precise. There is no unification among cybersecurity companies on how they deal with … And to say more, there are a lot of false-positives there. So what? They’re going to terminate our contracts because of some not very clean statistics?

The cybersecurity community should understand that it’s their responsibility to get organized, too, because without it in situations they see us as milking cows to monetize their services. Also, I think it’s time to question ICANN about the situation where the contractor’s party is demanding something out of contracted party because lots of guys from SAC have contracts with ICANN. They are paid by ICANN. It’s a situation where they create a self-fulfilling prophesies like, “Our income is low.” Okay, these things are dangerous and we are the only

company which can tell ICANN how dangerous that is. And of course, our consulting services are not for free. They're not doing it pro bono. Thanks.

DONNA AUSTIN: Thanks, Maxim. I think something to take out of that is what's happening on the DNS is perhaps a small part of the problem. There's a bigger, global cybercrime issue and unfortunately what I feel when we have these discussions within ICANN is that it's all our fault. I don't think that's the case. I think there's a small piece of the pie that we may be responsible for but within the community it seems to be, whether it's perception or reality, that we're responsible for the whole. Maybe that's a conversation we need to have about how we get the message through that. It's not all our fault. It's only a small part, perhaps, that we are responsible for or can do anything about. Can I go to Ken, first? Sorry. Yeah. So Ken, and then Jon.

KEN STUBBS: I'll defer to Jonathan for a second because he had a question.

JONATHAN FROST: Thanks, Ken. I've just got one very small point, at this stage, anyway, and that's that I'm not hearing a universal clamor for a change to the RA. I accept that that's one lever that could be dealt with but even from those that might be most demanding of some form of action I'm not necessarily hearing that they see that that's the preferred or only mechanism to achieve that action. Thanks.

SAMANTHA DEMETRIOU: Sorry, Ken. I don't want to jump you. I just want to respond that I think the one place we may be seeing that is potentially from the GAC because of their stated support for the CCT review team recommendations which did suggest exploring contract modifications. It's just something I want us to keep in mind.

DONNA AUSTIN: To follow on from Sam, if you have a look at the recommendations from the SSR2, they support the recommendations from the CCT review and I think there are additional things in there, as well. The statement from the BC is very similar to what the recommendations are from the SSR2 because I think there's somebody from the SSR2 that sits in the BC. Sorry. Ken?

KEN STUBBS: Yeah, I hope you can hear me all right. First of all, I'm somewhat turned around, here, and on a bit of a conundrum. I think we have a basic decision to make. Let's assume for the hell of it that the comment that Donna made about the fact that they're looking for some sort of a contractual change is a probability. We have only two choices. Do we let them decide what's important and what should be done about it or should we be proactive and determine based on our experience on a day-to-day basis what items are material enough to be discussed and make suggestions to resolve the issues?

I feel better with us holding the pen than I do with ICANN holding the pen because ICANN is much more subject to outside interference. We're going to do what we know is best and we have the capacity and the spokesman, here, to be able to … I hate to use the term "to see our story," but to make our case. I hope we seriously consider it. I don't like the discussion that points toward a fait accompli. Thank you.

DONNA AUSTIN: Yeah, thanks, Ken. I think the point that I was trying to get to is we do have to be proactive. We can't sit back because these review reports are out there. People read them. People take them seriously so we need to show that we understand that there is a problem, that we are doing certain things to address them to try to take a little bit of heat away so that when the board considers these recommendations they can say, "Well, we hear what you're saying but we can also see from contracted parties that they are being responsible in this area and actually doing things in the space." Stephanie?

STEPHANIE DUCHESNEAU: Stephanie Duchesneau with Google. At this point, I've only read the summary so there may be some flesh in the SSRT recommendations that is problematic. But one idea that I like coming out of it is this pivot from thinking about abuse in terms of individual reports and cases and up-leveling and thinking about systemic abuse and systemic trends defined by thresholds around the existence of abuse in a registry or registrar rather than what you do in response to an individual case.

I think dealing with individual cases you get into problems with how blunt the tools are, whether there are false positives, even if it is a correctly flagged report, whether it's the right way to be taking action. But when you just look at it in terms of abuse levels that becomes less problematic to me. I'm curious what other folks here think about the proposal to use incentives, maybe in the form of increased fees to parties that have higher instances of abuse. Because I do feel like there are players whose tools and pricing strategies do create a problem and aren't really internalizing the costs of abuse.

DONNA AUSTIN: Thanks, Stephanie. Brian?

BRIAN CIMBOLIC: Thanks. Brian Cimbolic, PIR. To Steph's point, I really like the CCT idea of the incentives. At PIR we have something called QPI. It's an incentive program based on a registrar's quality of registrations including … Domain name abuse is the first and foremost factor in that. We've seen registrars, that aren't qualifying in a way that they'd like to, come to us and talk about, "What can we do to get our abuse numbers better? How can we …"

There's a financial incentive behind it but it's an actor that wouldn't otherwise be focusing on abuse. That is because of the carrot dangling in front of them … Want to get better. I think that that would scale across registries, as well. The question is, would ICANN be willing to be the one that's providing the incentive?

UNIDENTIFIED MALE: Sorry. I just want to do a quick response to those last two points from Stephanie and Brian. Is that financial incentives recommendation in SSRT or in CCTRT?

BRIAN CIMBOLIC: I think it's CCTRT.

DONNA AUSTIN: It might be both.

UNIDENTIFIED MALE: Okay, I'm hearing that it may be in both. That's why I wanted to check. In a sense, it doesn't matter. It's not material but it's just more understanding so that others can accurately go back to the source of where the recommendation is.

DIETMAR LENDEN: Oops. Hi. This is Dietmar Lenden. I don't know if this has been mentioned yet but the SSAC started a working group, or a working team, to look at DNS abuse. One of their first tasks is to identify, and try an attempt to get, a definition of abuse. So, the team has started to get together last week. Friday, I believe it was. They are looking for people within the community to actually join their group, as well. I thought I'd just mentioned that.

DONNA AUSTIN: Thanks, Dietmar. Jonathan?

JONATHAN FROST: This is Jonathan from .club. In response to the idea of inviting either negative penalties or positive incentives for performing SLAs or contract commitments, just in general, I feel like once we open that Pandora's box every interest is going to say, "Okay, well, now it's a thing so we want to guide registry behavior by either giving them money or taking money away." Giving them money is really the same. You know, "Let's lower their fees," or, "let's raise their fees and then give them some of the money back." It all comes down to the same thing. Just opening that Pandora's box is so, so scary to me.

DONNA AUSTIN: Thanks, Jonathan. Seb.

[SEBASTIEN DUCOS]: [Jonathan, at this point] we live in a very strange world where there is "or death" as penalty. The one penalty that they have is to take away a TLD from us. There is nothing between this or death. If we start opening we're going to find a million use-cases for penalties given here and given there. I don't know that we want to get into that path. I don't know that ICANN wants to be that, either, because suddenly there is a completely different way of running compliance and everything that they run.

On Dietmar's point, the paper that was published in October and signed by a number of us that defines abuse, at least as it is comfortable to, would that be helpful? Is this something that we need to bring to them? Is this …?

DONNA AUSTIN: Thanks, Seb.

[MARK]: Hi, Donna. Hello? Is it on? Is it okay? I'll just talk real loud. How about that? Is it on? I'd like to push back on the comments about fees being a Pandora's box. This is from a historical perspective. When I look at where we're at with DNS abuse right now I actually see where we, as an industry, were about 10 years ago with domain name tasting. I see that same situation. And what everybody in this room should be aware of is a number of the lawsuits that were filed by contracting parties back then were filed by David Steele. If anyone read the Facebook lawsuit; David Steele. Okay?

Now, what was interesting is back then part of the carrot that ICANN gave to registrars was the fee reduction. To me, using economic incentives as a carrot is … I don't view it as a Pandora's box. I actually think it potentially could be innovative. It has been done once before. Perhaps, we could see how we can structure that today. I just want to give that historical perspective.

DONNA AUSTIN: Thanks, Mark. I've got Keith, Maxim, Brian, and then Rubens.

KEITH DRAZEK: Thanks very much, Donna. I'm not going to respond to the comment on the concept of fees or incentives, or anything like that but maybe taking it up another level. I think, generally speaking, we as the registries and contracted parties have recognized the need for further attention to DNS security threats/DNS abuse. I think we should and we have welcomed the discussion this week in the community and the engagement that we're seeing. Thanks to Jonathan for helping to shepherd that session, the plenary.

I think we've demonstrated that this is an important discussion. We welcome it and we look forward to being a part of it. I think we've also identified in the letter that we sent that better definitions of DNS security abuse are needed and that there's probably a role for the community in working through that. And that's, again, part of the discussions that we'll have this week and, certainly, going forward.

I think there's also a need for registries and registrars to develop best practices beyond what we've done so far and that, again, as we work together with registries, registrars, with ICANN, there's an opportunity for us to do that. I'll just, as an additional comment, note that, to the extent that we can develop best practices, that's something that could also be extended to our colleagues in the ccTLD community. Right? And so, it wouldn't just be limited to something, for example, a contractual change to the RA or the RAA. That would be much more specific to the gTLD space.

But at the same time there's a question of, are best practices enough? And should we, as contracted parties in the gTLD space, be considering an evolution to evolve spec 113b in the RA and other provisions in the registrar accreditation agreement? I think we as a contracted party house need to be thinking about, how do we want to handle this? It may not just be best practices or may be an evolution of those additional provisions in our contracts.

And then, I have a question from a GNSO Council chair perspective, and that is policy development. Right? We have best practices, bilateral contractual updates that could be made with potential community input or not. But then, what about a PDP? We could end up with pressure from a policy development perspective across the community to initiate a PDP. Remember, a PDP can also be initiated by the board by requesting an issues report.

I think we need to be thinking about, how do we want to look at this over the course of the next six months and a year, not just the discussions that we're having today? That's a comment that I also made during our ExCom session with the registrars so I don't think it'll come as a surprise to them that we need to be thinking a bit longer-term in terms of, how do we want this to play out as it relates to best practices, contractual updates, and the possibility of a PDP being initiated? I'll stop there. Thanks.

DONNA AUSTIN: Yeah, thanks, Keith. I think that was the third one that I missed that PDP is also a possibility. We might be happy about that because it delays

things but I think the important thing is we need to be seen as doing something right now, to the extent that we can leverage on things that are happening with other registries and potentially look at adopting that across the board. Then, maybe that's something we should give consideration to. So, I have Maxim, Brian, Rubens, and then Jonathan.

MAXIM ALZOBA: I have a few points, speaking about pricing. With anti-abuse, everyone says, "Okay, low pricing is bad," but we shouldn't forget about the regions where the income is, I'd say, way lower than in Northern America. What are we going to say, that you have to raise your prices so that your citizens are not able to buy your domains because it might be good, might be not? Who knows? I think it's a bad idea.

Also, a situation where ICANN is regulating effectively the policies, and at the same time is going to regulate prices will be an interesting subject for anti-monopoly committees all over the world. I'm not sure we need that as an ecosystem.

Speaking about the IDs, effectively they're turning anti-abuse into the vehicle for content regulation, which is a kind of censorship. I think there's going to be a clash between the local legislations and the definitions of what is good and bad. For example, involvement in regulations, etc. Sometimes one country thinks that it's a good idea to involve in elections into another country. They don't recognize it as something bad. Other countries think, "It's wrong. People are wrong," and it happens on both sides, or three sides, or four sides, many of them.

The last thing, about why it's going to be used. We had an audit and since the contracted party house has to be ashamed in full I think they will have an audit for registrars. I predict the same outcome where the loaded questions are going to be sent with a demand to deliver information they have no right to see. And then, to say, "Okay, both sides of the contracted party house misbehaved and here is the proof." It might be the moment to say, "Come on. To make it properly, first of all, you have to have good information." And in Yourdar, on which they based everything, it's shady and full of issues.

DONNA AUSTIN: Thanks, Maxim. I think the audit, at the end of the day, was a good result for us. I believe that, as a result of the process we went through, the registrars may not feel the same kind of pain. I think Jamie has learned his lesson. Well, I shouldn't put it in that way. But I think he's come to understand the importance of communication in these things so I hope it doesn't go down that path. I take your point about content and I think that's a conversation we've had before and were pretty clear on to Brian's presentation that he did in the pre-webinar. That sits outside what we think is within ICANN's remit. Stephanie, I still have you in the queue, thanks. Brian?

BRIAN CIMBOLIC: Thanks, Donna. A couple of points. I like Keith's model of thinking. You know, "What do the next six months look like? What do the next couple of years look like?" And I think it's important to talk about, "What can ICANN do now without modifying the contracts either through

amendment or through a PDP?" That's why I think an incentive is a potentially good idea because I don't think that would require contractual amendment.

There is also the option in the RAAs. For the purposes of DNS abuse, I think we can talk about registries and registrars together to some extent. The is a provision in the RAA that allows for termination if ICANN were to seek declaratory judgment that a registrar was knowingly permitting an illegal activity. There isn't an analog, here, in the registry agreement. I think that those are two things that we can point out that could be done now and that ICANN does have tools in its toolbox without going to the contractual amendment route.

What I would say is, to the extent that we are looking down either a PDP or a contractual amendment, I think a contractual amendment is the much more preferable route. I think if you look at spec 113b we're all under obligations to periodically search for abuse and take note of whatever action is taken. There is no obligation to take action. That would be, to me, a relatively easy fix.

There has to be some modicum of discretion and allowance for our policies, particularly to address things like compromise cases. If we identify abuse but it's a compromise case we shouldn't be under a contractual obligation to suspend that domain name. But my point is, I think that within the contract it wouldn't be that hard to get us in a place that we're all comfortable with and that would, hopefully, satisfy the community, too.

DONNA AUSTIN: Thanks, Brian. Rubens, Jonathan, and then Stephanie.

RUBENS KÜHL: Rubens Kühl, NIC.br. The feeling I have with including either financial incentives or disincentives is that these groups fought hard to remove price from the contracts. So, it's now not allowed in the picket fence to be defined. If you will open that avenue we might have other financial impositions imposed on us. I think this risk is high enough for us to try to avoid that, even for a good cause like fighting abuse.

DONNA AUSTIN: Thanks, Rubens. I think we need to understand a little bit more about what is meant by "incentives" because when I first thought about it I thought, "Well, the immediate impact could be on ICANN's budget and that may then have another impact back on us that they have to find the money from somewhere so where does that come from?" I guess that was my initial knee-jerk reaction.

But if it is a tool that addresses a problem that can take some pressure off us then maybe we need to think about it as, "Well, how would this work? And how comfortable are we with it?" Because I don't think it necessarily goes to the price point. I don't think it has any impact on that at all. But it's, "What behavior is worth rewarding or providing an extra fee on top of to try to clean your act up?" I think we need to understand a little bit more about what that is but I take your point. Jonathan?

JONATHAN FROST: Yeah, I'm with the Keith/Brian thinking that we need to be a little strategic and almost game-out, think how this is going to play out, and then try and respond to that. I understand what Brian said about potentially limited modifications to the contract but I worry with both the financial incentives discussion and the contractual modifications discussion that these may run away from us in the Pandora's box example. I think we need to go into that, if we do go into either of those kinds of discussions or considerations, with our eyes wide open that we may not control how it plays out.

And then, someone suggested something to me that I wouldn't mind hearing from others with more expert knowledge than me an opinion on. That is that ICANN isn't necessarily seeing or interpreting spec 113b in the same way as we might. There is opportunity for, perhaps, interpretation of that and a more effective enforcement on the back of the existing spec 113b.

There's a possibility, which I don't think I've heard discussed, of maybe an agreed advisory on the interpretation of that. So, there may be something which is not wholly contractual but nevertheless … That's an area I don't know if anyone's thought about, discussed, or had that socialized by anyone else. I'd love to hear some feedback on that. Thanks.

DONNA AUSTIN: Just two quick points. We have the PSWG coming in at 11:15. On the spec 113b, we will be having a conversation later today with Jamie and Russ on that. The final report of the audit called for a dialog on spec

113b so we're going to try to understand because we have a different interpretation of what it means than GDD or what Compliance does. We are going to start that conversation.

We do have the PSWG coming in at 11:15 and one of the reasons I thought it would be good for them to talk through the best practices that they identified in the pre-webinar is so that we can get a sense of what they think works and why they think it would address abuse. I think it would be a good conversation for us to have with them. That's why I'm leaning that way. Sorry for that. Stephanie?

STEPHANIE DUCHESNEAU: This is a bit of a jump back and forth because I wanted to respond briefly to the comments on pricing. I absolutely don't think that ICANN should be setting a price in the contract and that's not what I was referring to before. I think that's actually one of the advantages of looking at it in terms of thresholds because you're not prescribing the tool or manner in which you need to deal with abuse but you're acknowledging the fact that … Pricing doesn't directly cause abuse but if you're selling dirt-cheap domains that is correlated with a higher instance of abuse.

That's fine but then the onus on you is to put a different policy, process, or tool in place to deal with it. You can choose to deal with it with pricing or you can choose to deal with it through a different mechanism but you should just focus on the threshold however you get yourself below what we've defined.

DONNA AUSTIN: Thanks, Stephanie. I've got Maxim and then Jonathan.

MAXIM ALZOBA: A very short thing which is common for us and registrars. The first thing to be attacked, if the picket fence is removed, is premiums. In Rights Protection Mechanisms it was quite a strong attempt to attack it. We all should be prepared that if we allow that most probably most of us will be fired. Thanks.

DONNA AUSTIN: That might be an easy way out. Thanks, Maxim. Jonathan?

JONATHAN FROST: I guess I just wanted to bring up two points. I've heard some comparisons between us and the registries, and the registrars and the hosting companies, further on downstream. I guess we all have some responsibility to put policies in place that make the Internet a better place. But when I think about this, the further upstream you go the narrower of a vector you are and the more control over you have, but the blunter your instrument and the less information you have about the particular situation.

If we're a registry in the WHOIS privacy world we may not know who bought this domain. We may not who the customers are, what account came in, what it was paid with. We don't know anything about the hosting. We're not professional investigators. We run databases. The

registrar has the direct contact with the registrant. The hosting company actually has the content on their computer.

There are so many other parties that actually have the tools to make an educated and right choice so they don't create false positives and make the Internet a worse place by applying all these blunt instruments. I feel like we shouldn't accept these comparisons to registrars, hosting companies, and other companies that are in a better position than we are to monitor abuse.

By the same token, we have tools that we can do to make the Internet a better place but actually, we are the worst company in the world to actually decide. That's why when I get a court order it says, "Go to the hosting company. And if they don't, go to the registrar. And then if they don't, then go to the registry." We're the last person in line because we're the bluntest instrument.

Second of all, I feel like in our mission to make … As my second point, I think there are a lot of values, here, and one of them is protecting the consumer. That's a wonderful value. But we also shouldn't lose sight of the fact that due process and free speech is a very important value to all of us. If, in the proposals that we have, we make ourselves the judge, jury, and executioner, and we say, "Okay, we get a report from somebody who I think is pretty smart but I don't know him. He says this is spam. Okay, so I'm going to suspend the domain," that's really scary. Maybe we're doing too much there. Maybe there should be some due process. Thank you.

DONNA AUSTIN: Thanks, Jonathan. I think the points that you've raised we went into a little bit in the open letter that we had to say that we're just one in the ecosystem that can logically do something about these things. I think Brian's presentation was pretty careful in identifying what registries can and can't do. Then, the registrar. Ben pointed out what the registrars were able to do. I think part of the … Not challenge but part of what we need to build into this, too, is educating people about what it is we can and can't do. It is an ecosystem.

It doesn't, just because we're the registry operator, mean that we have certain powers to do certain things. It's not just as easy as to turn a switch. It's much more complicated than that. I think we've started that education process but maybe that's something else we need to factor in. I've got Brian and then Beth.

BRIAN CIMBOLIC: Thanks, Donna. I want to just touch on something that Jonathan mentioned which I both agree and disagree with in that I think we need to be really careful, when we're talking about abuse, of what we're discussing. Because the model that you described, Jonathan, I completely agree with, when you're talking about website content abuse. The hosting provider is where the content issue is most appropriately addressed because they have the ability to remove or get rid of the content and we can just knock down the entire domain name.

That model to me is not true when you're talking about domain name abuse. When you're talking about botnets, phishing, malware, then it's completely appropriate. To me, we have a responsibility to act on that

form of abuse. That's not a web-hosting issue. That is a DNS issue that we have an obligation, if not a contractual one, a responsibility to mitigate that abuse.

Just to make that point that, when we're talking about things being dealt with at the hosting-provider level, that's true when we're talking about website content abuse. But DNS abuse, I think, would not go over well if the registries and registrars were out there saying that this isn't our responsibility because I think it is.

DONNA AUSTIN: Thanks, Brian. Beth?

BETH BACON: Thanks. I just wanted, because we do have the PSWG coming in in about six minutes, to make a practical pivot. I think we clearly have a lot to discuss and we have a lot of expertise in this room. I think Keith laid out really well that it's a good idea for us to identify the three or four buckets of things that we could do. I also think that the Registries Stakeholder Group has a lot to offer here.

We should take control of our destiny in a way. If there are going to be best practices we certainly should have our head around what we think as a group. Obviously, we have a lot to discuss. Donna, I just want to suggest that we start putting at least pieces of this on our agenda so that we can get on the same page as a group or at least understand where we differ. But I think this is a really great start.

DONNA AUSTIN: Yeah, I agree, Beth. This is the first time we've had an opportunity to have a face-to-face discussion about this so I felt it was important. I probably should have given it more time. Jim?

JAMES GALVIN: Thanks, Donna. Jim Galvin from Afilias. Beth, I like that phrase of "practical pivot" because I think I'm going to call my comment that, too. There's a question that keeps coming up in my mind as I listen to all of these discussions about what we're doing and things that we might do. And I'm drawn back to the GDD Summit back in May when we were asking the question and this presentation started coming up in the forum. That is, what problem are we trying to solve? I think, Donna, you opened up this session with that.

So far, to date, most of our discussion has been about what we are doing but part of that is the education that we have to do. You asked us when we opened, "Where are we going and what are we going to do next? What's the part of it?" What that causes me to think about, again, is what problem are we trying to solve? We're being painted with a particular brush because there really is an issue in the community. I mean, there are DNS abuse issues. It's not at all clear to me that we're actually a part of the systemic problem if there is one.

I just don't understand that. I think that's a critical thing for us to consider as we think about things that we might do. There are a lot of good ideas that have come out on the table here for things to think

about. We need to ask ourselves why we're doing it. What are we trying to achieve? Who are we serving and for what purpose? Our contracts already have us doing things and we are, most of us, doing all of that. Again, "What problem are we trying to solve?" I think is an important question as we go forward to keep in mind. Thanks.

DONNA AUSTIN: Thanks, Jim, and I agree. But I think what we need to recognize is that because there's so much discussion in the community we do need to show what we're doing now. That's really important for us to do. It's hard to find ways to do that within this community. When we tried to find a mechanism for the open letter that was a real challenge for us. But I think maybe we need to start looking at the registry website and start to repurpose that for more useful information about what we're doing in certain ways.

But to the point about what problem are we trying to solve, from my understanding of conversations with ICANN staff it's what Stephanie was talking about. It's that what they want is some kind of prevention before it gets to the registration part; change your practices, change your behaviors. I think that's what they're getting to but they haven't openly said that yet. Quok?

QUOK PHAM: Quok from NeuStar. To the extent of what Brian was saying before maybe to help solve the problem we introduce a new term. DNS abuse remains with attacking or abusing the DNS and the new term that I just

penned down is “domain usage and content abuse.” If we separate that and we create a channel then maybe we can focus better on solving the DNS abuse issue and having the other stuff on the side.

IGFs are discussing DNS abuse in a similar way. They’re mixing content stuff with the DNS stuff. Ken, who is right there, has in his first statement about outside interference … That creates the outside interference and that bubbles up back to here. Maybe that’s something to consider, just better definitions.

DONNA AUSTIN: Yeah, thanks, Quok. It is really important. And to Jonathan and Brian, the conversation you were just having. We need to understand what we mean when we say “DNS abuse,” so we need to get better with our language. When we’ve had the conversations with Göran and he talks about bad actors we’re very sensitive. “Well, what do you mean by that?” Because it’s not the registry and registrar that are bad actors, in our mind, it’s actually the people that are using the domain names for the criminal activity.

Maybe what would be really helpful is that we do agree on what we mean by “DNS abuse” and then we can structure the rest of what we’re doing around that. I don't think we’ve firmly agreed that amongst ourselves and I think that might be helpful. Thanks, Quok. Sorry, JC and then Stephanie.

JEAN-CHRISTOPHE VIGNES: I think we are in danger of losing the communication battle. I think it's great to have a face-to-face meeting. We can have working groups and webinars and ask ourselves, "What are we trying to solve?" Meanwhile, the CSG letter was crystal-clear in what they wanted. Any Internet user could read that letter and identify the problem they are trying to solve. It's, therefore, very easy to demonize us, if you will. I'm not advocating a shortcut. I know we're [very extended] and the job being done so far since GDD is already remarkable. But I think we should not lose sight of the other side, for lack of a better term.

They are way quicker and way simpler in understanding than we are. Rather than having an educated discussion about what is and what isn't abuse I would love to portray us in a better, more practical way. To finish, not to pick on Brian, but when you said, "We have the responsibility, if not a contractual one," these words scare me to bits because the only responsibility we have is either contractual or maybe criminal. I don't think we should enter a moral area or arena because that's exactly what, again, the other side is trying to make us do. I think we should be really careful about what we project, here.

DONNA AUSTIN: Thanks, JC. Brian?

BRIAN CIMBOLIC: Yeah, just to respond to that. I appreciate the point, JC. But again, if you're taking that line then no registry would be mitigating DNS abuse. We don't have a contractual obligation to mitigate DNS abuse. We have

to monitor and report. There's no obligation to act and I don't think that that's a responsible model. I don't think it's a scalable model and I think it is a direct invitation to kick the door open into our contracts and have things change at a wholesale level.

STEPHANIE DUCHESNEAU: In response to the comment about definitions, I think it seems really natural that we should be starting with definitions but I'm actually worried that that's where we're going to get stuck. There are things that we can do without actually coming to consensus, necessarily, on exactly what abuse means, like incentives. If we looked at thresholds we could define it as narrowly as we wanted because the same people who have a high concentration of botnets are going to be the same people who have a high concentration in spam.

We can take something that's actually very narrowly scoped but does deal with a lot of the problem. I think the same goes for Brian's suggestions, as well, that we don't even necessarily have the be all in agreement on our definitions in order to make progress. I'm worried that we're never going to come to reconciliation on that.

DONNA AUSTIN: I agree, agreeing a definition is difficult. But I think we can agree the principles of what we're getting into and what we're not. I think we need to have some kind of scope as to what we're talking about. I think it would be helpful. Jonathan?

JONATHAN FROST: Just a couple of things. I kind of disagree with the idea that … It [flips around] that if we don't have a contractual obligation there's no reason, no prevention to prevent spam. There actually is an invisible hand at work, here. If a TLD gets a bad reputation mail servers are going to say, "Shut this down," and it's not going to have a good impression. We focus on .club as a global brand so it's very important to use that end-users see us as having a good reputation. There really are self-interest market forces in place. There are incentives to curb abuse other than contractual or moral. Yeah, thank you.

DONNA AUSTIN: Thanks, Jonathan. Welcome, colleagues from the PSWG. Come on down. Jonathan won't bite. Laureen, could I ask you to invite … What's the word I'm looking for? Introduce your colleagues, please.

LAUREEN KAPIN: Sure. Actually, I'm going to let my colleagues introduce themselves but I'll introduce myself first. I'm Laureen Kapin. I am from the United States Federal Trade Commission where I focus on consumer protection matters. I'm also co-chair of the Public Safety Working Group. I'm also participating in the Policy Development Process regarding the domain name registration system.

[CHABO BOFF]: Yes, good morning, everyone. My name is [Chabo Boff]. I work in the European Commission, DG Migration and Home Affairs in the Cybercrime Unit.

CHRIS LEWIS-EVANS: Good morning, everyone. Sorry, that's a loud mic. Good morning, everyone. Chris Lewis-Evans from the National Crime Agency in the UK. I'm part of the Cybercrime Unit in that. Also, I will always stipulate with, unfortunately, a member of the PDP for the GAC.

GABRIEL ANDREWS: Good morning, all. My name is Gabriel Andrews. I'm with the United States Department of Justice, FBI Cybercrime investigator.

GREGORY MOUNIER: Good morning, everyone. My name is Gregory Mounier. I'm working for Europol, the European Policy Agency, and the European Cybercrime Center.

[PERO QUIXEL]: Good morning, everyone. My name is [Pero Quixel] with the [Swedish National Police] here representing Europol [impact converting] child sexual abuse.

LAUREEN KAPIN: I know I also have colleagues in the room and I won't ask you to schlep up to the mic to introduce yourself but maybe if you could just stand and wave? The reason we're here is to engage with you so please don't stand on ceremony. You can catch us in the hallways as well as engage with us now in conversation.

DONNA AUSTIN: Thank you, Laureen, and welcome. We did have a conversation with the PSWG in a recent Registries Stakeholder Group call and we're really happy to see you here in the room today so that we can have some further dialog. We think it's an important partnership that, hopefully, we can work on, to some extent, certainly, the conversation around DNS abuse.

I think the fact that you and Brian took on the pre-webinar is an indication that we are in the forefront of the discussion. The more that we can have a conversation and get a better understanding of what our respective perspectives are then maybe we can work forward with solutions that are workable for both parties.

What we're going to walk through today … Laureen and I had a quick conversation in the hallway, yesterday. We thought it might be worthwhile going through … We've just had a conversation about DNS abuse and some of the ways that we can do a better job of informing the community of what we're doing and best practices was one of the things that came up.

During the webinar Laureen and some of her team identified what they consider to be best practices to respond to DNS abuse. I thought it might be helpful to go through some of those so that we can get an understanding from them about why they believe that these best practices actually address some of these concerns. I think that's good information for us and can give us a better understanding of the

problems that you see and how some of these best practices resolve that. Laureen, if I can turn it over to you?

LAUREEN KAPIN: Sure. I'll also be sharing the glory with my colleagues, here. I'm going to move this a little further back. We actually just came from a discussion with the GAC on this very topic. I also want to say thank you for inviting us because we welcome these opportunities to have a more informal type of discussion where we can share our perspectives.

We know we won't agree on everything. We know sometimes we disagree on things but this is all part of the process for hammering things out because within that universe of topics we cover we also know we're going to find some common ground and that that common ground has been identified in many cases. This is our way of trying to continue to find the places where we can move forward together.

In terms of best practices, some of the things we've heard about just this week have been discussed by specific ccTLDs. One of the things that we were actually focusing on just now was making sure that when someone is applying for a domain name that their identity is actually verified. Maybe I can ask Gabe to talk about that more because Gabe actually is on the front lines of dealing with cybercrime and has some very specific, real-life experience with what works and what doesn't.

GABRIEL ANDREWS: Hi. There are a few ideas. I'd like to say at the outset, though, we recognize that there are different majors that could be taken at the

registry level and the registrar level. Some of the things that we see and that we are encouraged by, proactive steps that we see folks taking, might be at the register level.

But I will note that there are registries within here, too, that have taken it upon themselves to incentivize that very behavior and that's also encouraging. When we talk about one of the most effective means of mitigating bad behavior it's removing anonymity. It is validating the registrant information. I'm not saying that's easy. I don't want to get into, necessarily, even what the best means of doing that is.

But I think we've seen some examples in the real world already, especially with the ccTLD presentation given by .dk where they have infrastructure in place to validate the end-user's behavior, or the end-user's identity behavior, improved. I don't know if anyone takes any position counter to that. I'd be interested in hearing any counter-arguments, perhaps out in the hallway at some point. But that's something that I firmly believe in.

We see some additional measures taken by others that perhaps can be taken at the registry level. Some of these are new; perhaps not even discussed by us yet, collaboratively. But I see bad guys, criminals, make use of domain look-alikes to craft spear phishing messages. We can call these homoglyphs, we can call them look-alike domains, but there are simple steps that some registries and registrars are taken to, when a domain is registered, also make sure that they block the easiest-to-identify look-alikes. Sometimes it's capitalization and what have you.

That's a nice, proactive measure. I don't want to get too prescriptive, though, because I think that as cops we're never going to know your space as well as you do. I think that you're in unique positions to come up with ideas to actually address abuse. What we're looking for is the opportunity to collaborate on identifying the best practices, sharing them, get behind them, and help incentivize them. That's where I see us to have grounds for communication and a reasonable path forward. That's my opinion and I invite others to join in.

CHRIS LEWIS-EVANS: Thanks, Gabe. I think I raised it in the meeting that we had with you at the GAC. For us, it's that sharing of that information across all the registries and down to the registrars, as well. You guys know your space. You know the best protective measures to take. Do you have a top-ten of, "These are the minimums that you should be doing"? It's sharing that across a community. We've worked with a number of you guys in here and that work has been really good.

But it's sharing it outside of ICANN and to all the registries and somehow enforcing that minimum standard and to create a minimum based on a standard that is viable for you to actually implement, as well. We're not blind to that fact. We can't say, "You must go and knock on everyone's door to validate them as a user." The viability of that is just …

That's where we are, looking to you to say, "Yeah, that's great," you would want that, "but really we cannot do it." We're not blind to those facts and that's where we want this communication to continue and

really help you … Is this worth doing? Yeah, of course it is. No, actually, that doesn't add anything. We want to be a part of that conversation with you and anything that we can do to help with any measures, then, yes, by all means. Let's say corridor, formally, however.

DONNA AUSTIN: Yeah, thanks, Chris. Best practices isn't something that we've gotten into too much on any topic. I think in the last few years we've been fighting fires just trying to get TLDs up and operating. It's been a bit of a lengthy process but I think on this issue we've just had a conversation that we understand we need to do more and we need to be, perhaps, more … Not even proactive in this space but do a better job of sharing information with the rest of the community that we are doing some things out there because we all have a responsibility and we all want a reputable product. We do undertake measures to deal with this type of behavior. Brian, did you have your hand up? Yeah.

BRIAN CIMBOLIC: Thanks, Donna. Brian Cimbolic, PIR. First, thank you guys for coming. I think the more that we can have these kinds of regular dialogs the easier it is to all be on the same page, not talk past each other, and really help facilitate encouraging dialog moving forward. I just wanted to briefly touch on the registrant validation piece. It's important to know, and it's not necessarily intuitive, but comparing gTLDs to CCs is a bit … It's not apples to oranges but it's kind of apples to crab-apples.

They have that direct contact with the registrant that we don't. I'm not even … What each specific model is for each specific CC. That's fine. But that's a really hard thing to copy and paste onto the G model. It's just something to keep in mind as you're looking at some of those country-code-specific practices.

DONNA AUSTIN: I know Greg will have something to say, also, but I did want to directly respond to that. I thought Gabe actually highlighted it well. We know you don't have the direct relationship with the registrant but you have contracts with the registrars who have direct relationships with the registrant and there are incentives that could be built in to reward good behavior by the registrars you have a direct relationship with.

I think it's that creative thinking. If we have a shared goal of saying, "Okay, we're going to do a better job of making sure the registrant is identified." And, "How can we do this, then, within our existing structures? How can it flow down? Can we provide some rewards and incentives? Can we provide some penalties or disincentives?" It's that sort of discussion that we think is worth having.

UNIDENTIFIED MALE: Plus, I think that's also a little bit what you're doing with the QIP program where you are providing incentives to your registrars to adopt best practices. But you're not able to implement them yourself because of the quality of the registry. But you can incentivize.

Something I wanted to say on the prevention side: we've been very impressed by some of the tools that some ccTLDs have developed in terms of recognizing malicious patterns of registrations. When you use artificial intelligence and machine learning it sounds really scary and it's very expensive but basically, they just correlate patterns and then it gives them pointers before a malicious registration takes place so that they do a double-check.

I was thinking that maybe, if the whole community is committed to preemptively make it harder for malicious registration to take place, we could also look into developing, collectively, these types of tools, making them available to registries if they want to use it. In the field of law enforcement, we have, for instance, in the field of cybercrime at Europol, we have a big database of forensic tools. These are free tools that have been developed by us with European money.

Any cyber community can use them. I think we could maybe look into the same patterns and the same system here where if EURid has developed this super-great algorithm that managed to identify malicious registrations in advance then maybe they could make it available for the community. That would be, also, a collaborative approach.

JONATHAN FROST: I would just say on behalf of my registry, .club, if there were free tools that are enterprise-level for investigating this kind of thing our ops team would just be thrilled to have them, on an API level.

UNIDENTIFIED MALE: Jonathan, just to those two prior comments. My understanding of that tool, just to be specific about it, and maybe you already know this, is it a pre-screening tool. It does a pre-screening algorithm and tries to identify abusive or other content. It's not a post-registration analysis. Both of which would be valid but just to be clear that that's what that is. It's pre-screening a text string and trying to identify whether abusive patterns are existent in it.

DONNA AUSTIN: Okay, so …

EDMON CHUNG: Edmon Chung, here. Sorry, I was just listening and there was one particular area that keeps me thinking in terms of better information-sharing and community because things that happen in one TLD might happen on others all the way from configure to TLD-hopping. Are there any thoughts, not only from our community but from PSWG, on thinking about how that may or may not work?

I'm thinking out loud, here, but if there are enough cases of this type of thing then maybe yeah, the registry community should really sit together and see how we can share information in a more consistent fashion to address those types of issues. I'm thinking way ahead of myself but this seems to be what's coming up, what I'm hearing.

JAMES GALVIN: A question that always comes to my mind when we talked about generally available tools for dealing with security threats, anti-abuse, or anything like that is, as we know, this landscape is an evolving landscape. It's essentially an arms race. Whatever we do, the bad actors figure it out and they get better at it.

The problem is if you become dependent on a standard set of tools then you also establish a baseline in which the bad actors just move on to something else. I just want to put that caution out there as we think forward to that. We need to deal more at a different level of concepts of what we're trying to achieve, not the solutions by which you do it because those things need to evolve, too. Thanks.

GABRIEL ANDREWS: Without getting too ahead of myself I will suggest to you that I, as an investigator and a liaison to an information-sharing agency in the US … It's just one of many potential means of sharing information but there exist organizations that are there precisely to help members of different organizations within an industry to share cybersecurity threat information with each other.

I don't want to pretend knowledge about other nations beyond my own. I don't have it. The organization I personally sit at is the National Cyber-Forensics and Training Alliance. It's called the NCFTA in America. It is there to allow investigators, both cybersecurity and fraud, to share information with each other and with law enforcement and it's one example that can be looked at. If you don't already have trust ops groups within your industry it's definitely something worth exploring. I

sort of imagine there are already communication channels that may exist for that.

When you're talking about sharing cybersecurity threat information whatever industry I've ever dealt with has determined that it benefits everyone to share that information. Especially within the financial sector I've seen first-hand knowledge in witnessing them evolve, there used to be this notion that, "Oh, well, it's a competitive advantage to keep this cybersecurity information to myself." That's been discarded.

It's to everyone's competitive advantage to recognize that you're team white-hat and team black-hat is out there victimizing all of you. I don't know if it's worth repeating and really hammering but as a point, it's very important. If you're going to benefit one person, I hope it did.

The second point I want to make is going back to what Chris said. We recognize that you are businesses. We want you to be efficient in your dealing with abuse. We want you to still be profitable and to be able to be good guys. We want to see that good behavior is incentivized. The bad guys are also businesses. We want them to be inefficient. We want their processes to be costly.

That's the end-goal, here. We want you to have all the incentives you need and all the tools you need and we want to take those tools away from the bad actors. If we can find any means of addressing those as goals, whatever the tools may be, and they'll change, I think those are admirable goals.

CRAIG SCHWARTZ: Hi. Craig Schwartz from fTLD Registry. Just to tack on to what Gabe was just saying. In the United States, there's an organization called the Financial Services Information Sharing Analysis Center. It's an ISAC. I know that the energy industry has their own ISAC and maybe it's time that we started thinking about some type of ISAC for us.

DONNA AUSTIN: Thanks, Craig. I think that suggestion did come up during the GDD Summit but I'm not sure how much traction it got. Probably because it got lost in a broader conversation that was happening. But maybe it's something we do need to have a discussion about.

[YURI]: We at Europol manage a number of stakeholder groups in the financial sector, in the Internet security sector, the Tenco. We work a lot with FS-ISAC and a number of others. I think from the law enforcement perspective it would be great if we would have an ISAC for registries where we could exchange [new modus apparently] of criminals registering stuff and then we feed it with you and you feed it back. That would be really, really helpful, I think.

DONNA AUSTIN: Thinking back to the discussion at the GDD Summit, I think some of the concern is, how do you secure that conversation? How do you do it within structures, [Yuri]?

[YURI]: Well, the good thing is ISAC have been around for more than 10 years so they have the technology, the CQ platform. At the end, you don't really exchange super-sensitive information. We can have the [mists] platform, for instance, which is really IOCs. We wouldn't be able to share operational information that are related to cases we're working on but the many IOCs that we can share that can really help.

Yeah, the CQ platform. We have a number of CQ websites where we share information and then we've got face-to-face meetings regularly. Really, the point is to create trust and to know people. A little bit like ICANN, but that would be focusing more on security and cyber-threats, I think. Taking the step is already in the right direction, I think.

LAUREEN KAPIN: Just in a very practical perspective, our agency has law enforcement partnerships with our colleagues across borders. We deal with exchanges of information to work better together but that's not a concept that certainly couldn't be adapted to any sort of strategic effort where you're exchanging information about trends you're seeing. "We're seeing this trend, how are you dealing with it? This is how I'm dealing with it." That doesn't necessitate or require sharing super-sensitive information. It's more a top-level, "Here's what we're seeing and we'd like to engage with you on how to deal with it," failures and successes, at a very simple level. I think that sort of dialog can be very helpful.

UNIDENTIFIED MALE: You have access to advances in technology that many people are not even aware of yet. Given what we would expect to happen in the next 10 or 15 years, this shouldn't be an esoteric idea. This should be an absolute necessity. We can take this to power grids and get very specific but there are so many things that, over the next 10 or 15 years, could be drastically affected if we don't put in place the ability … We have to start looking further out. You can't just live with a good idea. You have to step out and take the chance. You have to put the resources out there. And every once in a while, something isn't going to work. But when it works it's really going to make a difference. Thank you.

MARTIN SUTTON: I'm liking the discussions and the way it's starting to lead because it does resonate with the financial industry from the past and the growing fraud issues that emerged as online banking services switched customers onto that platform. The amount of effort to get people together is immense. But when there is a commonality between what are traditionally your competitors it adds a really good value because then you start to look at the aggregate issue, rather than the activities that you're all doing individually, which you may think are controlling, at least, your problem to a manageable level.

But when you look at the industry – and I think this is the issue that comes about, here – the view from outside is that the industry itself as a whole is not being proactive. Getting together and being able to define some of the issues, start putting numbers or statistics together that are meaningful on an aggregate level, start to prioritize where you

address some of these issues and bringing together some of the expertise. That would be from law enforcement but from the business sector, as well.

Actually, it makes the problem-solving element a lot, lot easier and you can start to see results in a reasonable amount of time. It doesn't need a huge investment in technology, either. There's probably a lot of it already spread across that exists, now.

BETH BACON: Thanks. At this point I think we're probably piling on a little bit but much agreed with Martin. We've talked a little bit in our time, without the PSWG here, about what the SG can do more as a resource, as a group of experts. I think information-sharing, at least among us, is a very easy thing for us to do and could be really practical once we do have that tool where we could go out there and it could contribute to a best practice or just basic knowledge. Maybe that's something we could think about for the SG.

It came up, also, in the GAC session when we presented requests for, "How do we share amongst ourselves?" I think even in our discussions it has become clear that sometimes we don't. I would support that and think that we could take that on as an SG.

DONNA AUSTIN: Yeah, I agree, Beth. I think a lot of our focus is, "What do we do within ICANN?" and that's what our conversation is about. But we don't really talk about the operation of the businesses and what we do on a day-to-

day basis. I think I'm starting to get the sense that that would be worthwhile, to use the stakeholder group as a means to do that. That's a little bit of work that we have to take on to change that posture a little bit. It's not something we've done previously but I think we could do it in the future. Martin?

MARTIN SUTTON: I think that's a good starting point to get commonality amongst the registries and start from there. I think you've also, perhaps, got some vehicles available already that stretch beyond the Registries Stakeholder Group and sits outside of ICANN. Something like DNA might be an area where you pull together other expertise and connected parties. If there is an interest to do something, that could be a conduit for wider than the Registries Stakeholder Group. And perhaps the Registries Stakeholder Group becomes a member of an organization or association like that to feed in.

DONNA AUSTIN: Of course, you always have the BRG and the GeoTLD group as well. I think it might be helpful to bring them in as well. They aren't members of the Registries Stakeholder Group but we don't work the other way. Yeah, we do have some structures that we could probably use, already. Maxim?

MAXIM ALZOBA: I have a question for members of the Public Safety Working Group. Do you see the DAAR tool currently advertised by ICANN as a proper vehicle

to measure the abuse [liable]? For example, all it gives to registries is just a number. For example, "Today, you received five." The next day you receive three and you don't even know what it means.

The second question is, we've seen false positives there, where the information was not checked, or information about domains which never existed in the DNS system. But maybe someone used it in some coding and some of the sources on [full ought] included it into the report for the particular TLD. And they have nothing to do with that particular case, for example. Thanks.

MARTIN SUTTON: Realistically, for us, I think DAAR has two functions. The first function is to enable us to be able to talk about the abuse that is happening across the TLDs. As a vehicle, if you just ignore the numbers and everything else, the stats that come out, the reports that come out, aren't brilliant but they're a good way to start that conversation. As a vehicle for starting the conversation and start that communication I think it has been quite effective. I would maybe suggest we wouldn't talk about DNS abuse constantly, it seems, here, if it hadn't have been for DAAR.

As a vehicle for starting the conversation, I think it has actually been quite good. But what you're provided with from DAAR … Obviously, we don't see what you're provided with. However, we've had conversations and I don't think the level of detail that you're getting is enough. We've asked, and I think it's in most of our slides, that we would like that to be as public as possible and for the data that comes out of that to be more granular so that you're able to take better action.

On your third point, yes, there are problems with it. I think we see those problems, there. Some of the verification side of the abuse feeds, it's not there. It is just a simple aggregation of different data feeds. And how do you confirm some of that? That's not done in the DAAR at the moment. Could it be done? Yes, definitely. There's no reason why you couldn't take the DAAR and then add extra verification steps on top to improve the quality of the data that you're getting from it.

Is the data good? I think yes. Is it complete and 100% accurate? No. But I think there are questions that we can ask of ICANN to improve some of that. Some of that may be having to open up mechanisms of sharing your data with the DAAR tool to enable them to make more accurate decisions based on that data. I think, as we are now, that some of this communication that we need is, what do we need to give you that verified and accurate information from the DAAR tool? How do we complete that? What are the best practices that you can glean from it?

DONNA AUSTIN: I think Jim or [Christian] might have some further … Yeah.

JAMES GALVIN: Thank you. I think that, yes, the comments that you're making about future conversations and future discussions are good and important. We have actually been talking ourselves. We have a DAAR Working Group, ourselves, within the Registries Stakeholder Group. We're actually working quite closely with the OCTO team on what we can do with DAAR to evolve it to a different place, to a better place.

I want to react, I think, on two things in particular. It is important to continue, for Maxim's comment, to understand that DAAR today is not an actionable presentation of information. It's important to understand that. At best, it's a leading indicator of the location of some abuse. But you made the comment that registries or other parties could take on what they see in DAAR and then go and do something about it and the reality is that you can't. That's the point that Maxim is trying to point out.

DAAR might be a leading indicator, informational, with respect … But it's not directly actionable and I think that's the careful point, here. The registries would still have to do their own investigation and research and go find stuff.

There is the second question about the quality of what DAAR represents and there are a number of issues, there, one of which is the quality of the input that DAAR gets as part of what it does. I just want to call out that that's an important discussion going on in our current sub-group where we're working jointly with OCTO. We're working through that so that, we hope, we can get to a place where what DAAR presents is much more informative and much more useful to the community.

It still may not be actionable in and of itself. That's an area to be explored and it is an open question. I do want to be careful about declaring that DAAR is in any way a high-quality resource. It's important just to temper that presentation about it because that's a very important topic of discussion between us. Thank you.

UNIDENTIFIED MALE: We understand that and we don't promote DAAR just because it's DAAR. From my perspective it's important that in the community there is a consensus that we need to have transparent and efficient tools to monitor our views, at your availability, that you can use, that is actionable and everybody. It can be something else. The point I wanted to make is the registries are really managing a critical infrastructure. I think the regulators are understanding that more and more. For instance, in the European Union, we've got the NIS directive.

We mentioned a number of actors and they mentioned the DNS operator as possibly being critical infrastructure managers or actors who need to take specific actions. Having these tools to monitor abuse for the industry is essential. Getting organized to share an indicator of compromises is absolutely essential.

This is a sign of a mature industry that is conscious that they are managing something absolutely essential for our society. I think it's a no-brainer that you should have these types of tools, being DAAR or other ones. I think that's really the message that we are pushing. You have a special responsibility and it goes beyond just a competition, the market, and the rest.

DONNA AUSTIN: Maybe that's a good conversation for another time because I don't think that we necessarily see our respective operations as critical infrastructure. Chris, did you want to go first, or Alan? Alan and then Seb.

ALAN WOODS: Thank you. Pardon me. Clearly, I haven't talked yet today. I just wanted to say I think it's very great to hear the information and the dialog that is happening here today. I think it's very important to know that there are a lot of actors who we are hearing this and we hear all the information that's coming to us. We are actively, on a day-to-day basis, struggling with our position and the expectations placed on us specifically as registry operators. Sure, there are a lot of us around this table who would absolutely love to be able to be the hammer. But unfortunately, we are not the hammer.

I would bring to mind things such as the Internet and jurisdiction and the showing of the scale, of where we sit on that scale, and finding the sweet spot that we can work and we can work effectively with people. Again, it is very difficult. I'm glad to hear the appreciation that it's not as simple as just going to the registrars and the registries and saying, "You must do this." It's about accepting that you must do what you can in your position given the circumstances and the availability.

Again, we are private companies. We get a lot of pressure from outside people, as well, saying, "You shouldn't be doing this in your particular area. You are not the police. You are not this." Again, that's another good thing to hear, the understanding of the expectations placed upon us. I, for one, and especially from Donuts, definitely want to be able to play a good part in this. I think it's just finding that specific niche role that we can act effectively, efficiently, and of course within the

boundaries of the law. I think that's an important thing. I just wanted to put that on the record. Thank you.

SEBASTIEN DUCOS: Sebastien Ducos, NeuStar. Just bouncing on. We don't see ourselves as infrastructure. Our friends from the ccNSO definitely are and we are on our way to being it. We need to look at it that we. NeuStar have a client in Italy, that I won't name, that is going through that process today. I don't know what the situation is with a brand like [a sincere] but when the national operator runs all their commercial operations for us we are infrastructure.

DONNA AUSTIN: Chris, and then JC.

[CHRISTIAN]: Just one clarifying point and one thing that I just don't believe that Alan said is I do not believe he's not spoken yet today. The actual point is Jim's comment, what I was referring to about taking action. Yes, I don't believe you can take action off the output from DAAR but the information underneath DAAR that you don't have access to with extra steps that's when we can start to take action. Just to clarify what I meant by that. Thank you.

JEAN-CHRISTOPHE VIGNES: [UNI] registry. Just coming back to what Sebastien just said. The NIS treaty mentions critical infrastructure and the keyword here is

"critical." Some ccTLDs, some governments, may decide that ccTLDs are a critical infrastructure. That's the case for .fr. But it's not automatic and the fact that some of our clients may require us to abide by some rules that may make us a provider of critical infrastructure does not automatically make us providers of critical infrastructure with all the consequences that the NIS treaty would attach to it. No, we are not. We are, for the most part, private providers with some contractual obligations. Thank you.

DONNA AUSTIN: Thanks, JC. Jonathan, do you …?

JONATHAN FROST: I suppose I'll follow on from JC. I think these are nuanced legal/technical points. Also, the concept of infrastructure, even, and what that means. I mean, it's a useful discussion but we need to be careful about accepting definitions of national, critical infrastructure and what those may or may not mean because they certainly aren't universal standards at this stage across the TLD industry by any means. Thanks.

DONNA AUSTIN: Okay, thanks. Laureen, do you want to draw a line under this?

LAUREEN KAPIN: One of the things that we did want to acknowledge is some of the good work that has already been done. We realize this isn't uniform and we're

not saying it necessarily should be or everyone has accepted this but one example is trusted notifier programs. I know some of the registries in the room have this. And this is a great concept for providing, basically, efficiencies as a result of some groundwork and common understandings where you have this dedicated path that makes things go more quickly and can have a targeted result and an expeditious timeframe. That's a great concept.

One thing to explore is, can there be some partnerships with particular law enforcement agencies that deal with certain things on a routine basis where it would be fabulous if we [got marry up] platinum category service because we went through the groundwork of figuring out what you need and how we can get it to you. That's certainly something that could be explored just by way of an example.

I would be remiss if I didn't acknowledge that the framework to address abuse was a very welcomed effort. I know not everyone agrees with that and I know not everyone has signed onto it but the work that was done to come up with common areas of understanding and categorize things into "must," "should," "would be great if," and I'm paraphrasing, of course, that's great work to start doing and start thinking about.

We want to encourage that sort of thinking. We also realize that when you come up with something like this it's voluntary and is different from rigid standards. We want to reflect that we definitely understand the difference. Those really fall under the whole category of best practices. Gabe? Oh, yeah.

JONATHAN FROST: If it's okay to get back right on this a second. Especially as regards trusted notifier, I need to get a talking point out before we run out of time. My country in particular, and law enforcement therein, deal sometimes with the seizure of very large numbers of domain names that are associated with botnet command and control. In particular, in recent years some colleagues of mine have been dealing with the avalanche botnet which had hundreds of thousands, if not approaching millions, of domain names. Thank you, 800,000 says my colleague.

This is, of course, domain names that are generated by a domain generation algorithm wherein those names are only relevant to the bad guy for a very particular time. Maybe a day. Maybe hours. I don't know the details but a very concise period of time. We in the criminal justice system have tried a mechanism of going through the courts to say, "Well, predictively for the next year, what are all these domains going to be?" and trying to update that year-by-year. We are quickly coming up with the realization that our criminal justice system is not able to sustain this pace. It is not going to be viable for us to continue to do this.

We need a mechanism, perhaps this is a trusted notifier program, wherein we can come to you and say, "Hey, we're working with computer scientists, researchers. We've cracked this DGA. We know what the domains are going to be. Here it is. You can use this and see which ones are coming up and take action on your own." But I can tell you now, it is not going to be viable for us to continue to use the courts for this methodology.

And so, this is a conversation I think you need to be ready for. It's already ongoing with some. I don't want to get too in the weeds but I just need to make sure that we're clear on this point that sometimes this is the best way to deal with threats. It's to come together and talk and not rely upon just court order.

KEITH DRAZEK: Thanks, Donna. Hi, everybody. Keith Drazek. In the context of trusted notifiers and best practices, as I said earlier before this portion of the session, we think there's more that registries and registrars can do with regard to best practices. We think a trusted notifier approach developed through an ICANN-convened process is probably an appropriate way forward.

DONNA AUSTIN: I'm not sure what that would look like to an ICANN process, but anyway. Brian?

BRIAN CIMBOLIC: Thanks. I just want to touch on, briefly, something Gabe mentioned on DGAs. That is a bread-and-butter DNS abuse issue in my opinion and one that I would encourage everyone to work very cooperatively on, to the extent that a DGA has been identified to work with law enforcement when they've made that identification. The one thing I would say is for us to go down the route of working on DGAs without court order …

Because at PIR, at least, we would certainly act on DGAs without a court order except as far as there's a contractual prohibition of us creating domain names not through a registrar. When we get a DGA that comes in by a court order we go to ICANN and we get permission through something called the ERSR.

I am certainly comfortable acting without a court order on DGAs. But that requires ICANN, there, hand-in-hand, saying, "Okay, you're allowed to and you don't have to pay fees on these [creates] that you're doing to mitigate abuse." I imagine they might be cooperative and come to the table in good faith on that but that's just something that we would have to work into that process.

KEITH DRAZEK: I feel confident we can have productive conversations to that effect.

DONNA AUSTIN: Just moving on, and I'm mindful of the time because I don't want you to be late for your picture. The other thing we briefly wanted to touch on was the status of the Expedited Working Group on Domain Name Registration. I think one of the big issues that we're concerned about is that as the Policy Development Process continues, and the implementation process continues, we know that there's going to be a time lag between the time policy concludes, implementation concludes, and then actually everything gets built and created, that that's just not magically going to happen instantaneously.

What we are concerned about is making sure that in the interim the policy that we do have on the books, in terms of reasonable access, actually is working properly. We wanted to underscore that that is a concern of ours and that perhaps there can be productive work on how to make sure that, basically, people know – and when I say "people," I include especially, of course, your authorities tasked with protecting the public interest – that folks on the front lines know they can request this information, that they know how to request this information, and that if they're not getting this information when they should that there's a mechanism to address that.

I'm just sharing with you that that is really a big concern because what we're hearing from our colleagues is that there's this information gap and sometimes that requests are unreasonably denied and there isn't reasonable access. I'm not really pointing fingers or asking for folks to solve this problem. I'm reflecting on what the problem is and saying that there's work to be done.

I think the ICANN Organization and registries can certainly have a role in figuring out how we can make sure that this process that's currently in place is going to keep us going until whatever permanent system we agree on is in place and that we need to make sure there's a safety net here so that things continue to work.

ALAN WOODS: As I've been activated by Chris, I can't stop talking now. I may be shot with a shovel – which is a very good Irish saying, here – for saying this but there are a lot of people around the table, here, who have the

processes in place and we have the portals and the platforms. Perhaps this could be a member thing that we put together a handy sheet of how each registry at the table, here, does take such requests in. Just as a little bit of a stop-gap measure at the moment, a sign of good faith that we are there, we have these processes in place, and maybe just a little olive branch in that one.

LAUREEN KAPIN: And we love olive branches.

SEBASTIEN DUCOS: Just to complete that, and maybe not on-mic but off the mic, if you do have examples, if you have people that complain, just tell us and let's look at them. Because, particularly with the ePDP Phase 2, we're going into this massive construction of that final solution that, as you rightly say, is getting so big that it will take time not only to policy-develop but then technically implement.

I'm not even confident that it is something that we will be able to technically implement in the end. Let's demystify and let's find ways of finding ways to find solutions. Most of the registries I speak to talk about units of requests per month, about things that are completely manageable by us. The things that we are able to take care of as it is. If there is a problem, let's find it.

LAUREEN KAPIN: Yeah, and I welcome that. I mean, I personally have private conversations, and that's one of the things that's great about these interactions in the ICANN ecosystem. It's that you develop these relationships and you can say, "Hey, I heard this request was denied. Can you share with me what the problem was so I can work with my colleagues?" Yes, absolutely, we will do that.

UNIDENTIFIED MALE: Really just 30 seconds. We have started an initiative with the registrar where we are gathering a law-enforcement point of contact for each of the registrars and we're putting it on a platform for law enforcement only. And we're educating the law enforcement community of, "If you have a problem or you request information then do this, and this, and this." So, we've got profiles on registrars. I haven't thought about actually engaging with you guys but maybe I can speak to you and then I'll circulate a call for sending us information facilitating the contact? I will do that.

DONNA AUSTIN: I think we're at time so I want to say thank you. I'm encouraged by the tenor of the conversation. Sometimes things get heated and volatile and that's not what this has been. I think this has been a very reasonable, constructive dialog and engagement and we welcome these opportunities. Again, you can approach us individually, one-on-one, to further the conversation. I thought I saw a hand up. Yeah?

SEBASTIEN DUCOS: Yeah. Speaking on behalf of Steiner from .global who's not present but is asking, do we know … And I know nothing about it so I don't know if there is an answer, but do we know how many people are actually implementing the ICANN-provided API? The MoSAPI from DAAR? Is anybody using it on the registry side? We were not. We have our own solution that is independent for it.

[LAUREEN KAPIN]: Someone's going to have to keep me honest on this. I don't know that the data provided through the MoSAPI is specific domains. I think it's like "counts." It's still not actionable, per se.

SEBASTIEN DUCOS: Okay, I'll assume that he accepts the answer.

DONNA AUSTIN: Thanks for flagging that, Seb. Sorry. So, Laureen, thank you very much for coming in. I agree, this has been a great conversation and that's the way I'd like to keep it. A conversation. We meet every other week so if there's any topic that you ever wanted to discuss with us we are happy to get you on the agenda so that we can have that conversation. It doesn't just have to be here at ICANN meetings. We meet pretty regularly so we're happy to get you on the schedule if there's something you want to discuss. Likewise, I think if there's a conversation we're having where the input from you would be valuable we'll reach out and make that contact. Yeah. So, thank you. This has been great.

LAUREEN KAPIN: Thank you.

DONNA AUSTIN: Thank you.

[LAUREEN KAPIN]: Okay, some logistical information. We're going to break and take a photo. You'll need to go out the door, turn right, and you'll see the little photo spot. It's like a tiered setup. That's where we're going to take our group photo. Then, we'll come back in for the buffet lunch. As in the past, the people that responded are the ones that get to eat, okay? We have about 70 people that responded so we really need to push through and get this done because we've got a very packed afternoon, as well. Please, quickly move into the hallway for the photo. Thank you.

[END OF TRANSCRIPTION]