BRENDA BREWER: Hello, everyone. This is Brenda speaking. Welcome to the BC membership call on 4 April 2024 at 15:00 UTC. Today's call is being recorded and is governed by the ICANN expected standards of behavior. Please state your name before speaking and have your phones and microphones on mute when not speaking. Attendance is taken from Zoom participation. I do have apologies from David Snead, Tim Smith, and Vivek Goyal. With that, I'll turn the meeting over to BC Chair Mason Cole. Thank you.

MASON COLE: Thank you, Brenda. Good morning, good afternoon, good evening, everyone. Mason Cole here, Chair of the BC. Two minutes past the hour on April 4th, and thank you very much for joining the BC call today. It's good to have -- we have a nice critical mass of BC members on the call, which I appreciate. We also have our Non-Contracted Party House board member, Chris Buckridge, with us today. Chris, thank you for joining. I understand you can only stay for about 15 minutes, but we appreciate making time for the BC call today.

All right. The agenda for the day is on the screen. I do have a quick update, which is that Tim Smith is unable to make the call today. Therefore, we may skip item 4 on the agenda, and I will solicit from Tim an update on finance and administration and provide that update to the BC over the list. But are there any other updates or additions to the agenda before we begin, please? All right. Very good. Okay.

So we're going to go right to item number 2, which is a presentation from the DNS Abuse Institute. Our friend Graeme Bunton is our guest today. Graeme, thank you for joining the BC. We've asked Graeme to provide an update to the BC on what's happening with the DNSAI, in general, what's happening from the contracted party perspective on DNS abuse mitigation and whatever color Graeme would like to add to that conversation, which will be informative because he's obviously an authority in the space. And Graeme, I believe we've got about 15 minutes reserved for you, plus some time for Q&A. Will that work for you?

GRAEME BUNTON: That works just fine. Thank you.

MASON COLE: Very good. The floor is yours. Take it away. Thanks, Graeme.

GRAEME BUNTON: Well, first, thanks for having me, Mason. I really appreciate the opportunity to talk to the BC. It's not every day. I'm going to share my screen, and I'll try not to talk too quickly. But there's a bunch I want to get through and make sure that I've got room for questions. So I'll do a very brief intro, just in case I'm a new person to some of those on the call. Then we'll go through the work we've been doing on Compass and NetBeacon and talk a little bit more about how this audience can engage, hopefully.

Briefly on who we are, the DNS Abuse Institute is a project of Public Interest Registry who operate the .org TLD. PIR is a not-for-profit, and making the internet better is part of their not-for-profit mission. And so they spun up the Institute to try and continue doing that work, especially as it relates to malicious domain registrations. The Institute doesn't do anything related to the registry operation itself. We don't look at PIR's abuse. We don't look at the PIR's business, really. I sometimes describe us as being incubated by PIR, if that's helpful. And I say that just because I want to make sure that people see us at least as functionally separate from the registry and that our work is always trying to be as sort of independent and rigorous as possible and not bring any particular contracted party perspective to the discussion.

But really, our work is to try and reduce malicious domains across the ecosystem, and we're doing that by a couple key projects. I'll talk about two today. The first is Compass. This is our measurement project. It's similar in some ways to ICANN's DAAR, but I would argue significantly more advanced, which is fair enough. DAAR is like 15 years old or something at this point. So Compass is really about benchmarking the prevalence and persistence of malicious domain names, of abusive domain names in general, but really focused on malware and phishing as those have the best datasets available for them. It was really important for us as we launched this project that it was credible and transparent and accurate. So the credible and independent is we hired an academic to do the work for us. That's Maciej Korczynski out of the University of Grenoble, and gave him a brief of measure abuse the very best that you possibly can. The methodology for this is entirely transparent. It's published on our website. I've got a link further in this

presentation. And accurate and reliable. And so we know there's more abuse out there than what we're measuring inside of Compass. But what we're measuring, we think is as correct as it can be.

We measure phishing and malware, as I said, we measure mitigation rates so that we can see if a harm is no longer available online. We measure the speed of that mitigation. And we split these registrations between malicious and compromised. And those things give us a pretty robust dataset. We do this across all registrars and TLDs, both CC and G.

So we have public reporting on our website, you can go see some sort of high level trends, we tend not to editorialize about those trends. You know, we've got about two years of data up there now. But I don't know that it's particularly meaningful to say that abuse is going up or down, so we don't. But what we have started doing, and one of the things I wanted to highlight here, is that we started producing specific reports. These are inside of PDFs, they're pretty long, they're pretty dense, we're very careful in our wording. But we do name registries and registrars that both observe low levels of abuse and high levels of abuse. And I think this is something that community has been really interested in for a long time.

And so I've got, boy, an awful lot of text on this slide, but two tables. One is for registrars with low levels of abuse. I believe it's malicious registrations per new domain registration. And so that to me is a really good metric of how much abuse a registrar is driving. And on the other end, we have the high rates of abuse per new registration. And so you can see that [inaudible] is number one there, Alibaba is Singapore, number two. It might have been that Alibaba cred that was just

breached by ICANN Compliance. They have four creds, I'm not sure if it was that one in particular. [inaudible] is there. You'll also note that there are some redactions. We only name the registrar TLD on the high levels of abuse if they're in that top 10 for four of the previous six months. We do that because we've seen quite a few registrars and TLDs that are impacted disproportionately one month and then not the next, or for two months and then not the next. And what we're really trying to highlight here is consistency. And so if you're interested in this data, it's available on our website, please go check.

The big thing though, that we're working on this year for this project is measuring the amendments, the impact of the amendments. And we think because we have two years of this really robust data, that we're in a very good place to do that. And so we're spending a lot of time right now thinking about what's going to happen in this new context and how we're going to measure it. So how are the concentrations of malicious domains changing? Do we see a movement from Gs to Cs because the ccTLDs don't have these requirements or not exclusively? Do we see more abuse move to subdomains, which is sort of outside the purview of ICANN in this way? Do we see more compromised websites? Do we see more abuse in blockchain and alternate root domain name systems? Things like that. Do we see the time to mitigation come down? Because that's a stat that we've been measuring for quite a while. So are registrars getting better at acting faster, which I think is a really important measure. And then how are overall mitigation rates changing? Are our registrars able to mitigate more abuse than they have been historically?

And so those are sort of the sort of broad strokes way that we're thinking about measuring the amendments. We're pretty publicly committed to doing that for the community. Boy, is it tomorrow? Alan's on the call. I think he might know. They come into effect tomorrow. And so we hope to get some of this out in the nearest future so that people can see these trends as they begin to happen. But it's a bunch of work running a project like this. And we try to be extremely careful in how we present this data. But please stay tuned for that as we get it out the door.

I'm going to go very briefly through NetBeacon now. And then I'll take some questions. NetBeacon is our centralized abuse reporting system. It is free. It's pretty easy to use. It allows anyone to report DNS abuse to any gTLD registrar. We've been operating that for about three years now. And it's been, I think, so far, a pretty successful experiment. And perhaps just as a side note, this sort of thing was in a bunch of different ICANN outputs from the community. So SAC-115, SSR2, and a couple other things sort of said, boy, it would be great if we just had this centralized system to report abuse. We've built that. We think it's working and fulfilling that gap pretty nicely. So anyone can use it. You can go use it right now if you feel so inclined. Please do.

In 2023, we saw some 23,000 reports of abuse go through it, almost exclusively phishing, and I would say split about four-fifths through the API and about one-fifth the web form. So I think institutional reporters versus general public, which is probably about right. My sense is that it will always be more heavily used by what I would call an institutional reporter.

We monitor deliverability. Unfortunately, the industry still primarily relies on email. And so we're keeping an eye out for bounces and things like that. Deliverability remains high across the ecosystem. Quality of the reports generally remains quite high. We don't manually review what goes through it, but because of the friction, the forms, and the API put in place, the quality of the reports is generally pretty good. We began integrating ccTLDs last year. I have about 10 of them on board, and so that we can now accept abuse reports for those ccTLDs as well. And then we're continuing to work with CleanDNS, and a big thank you to them for supporting this work on new features. The forms that we have for NetBeacon are embeddable. It could be in a place shortly where anyone can put those forms on their website, and why not allowing anybody to report abuse from anywhere? And then working on reporting abuse to web hosts and other infrastructure providers at the same time so that we can try and disrupt online harms at both the web hosting front and the domain name front. Or if it's a compromised website, get that report to the web host where it belongs in the first place.

And so I'm so far very happy with NetBeacon. There's so much work to do to continue making it awesome and continue routing abuse. My key goals this year are really to drive more usage. And that gets me to how this group can help. I'm very interested in thoughts and feedback on measuring the impact of the amendments. If we've got the data, we'll try and do it. So don't be shy about your ideas there. Use NetBeacon, try it out, give us feedback. We don't think it's perfect. We always want to make it better. And so participating there is helpful.

And then help us close the loop with organizations with high-quality abuse data. We're very interested in talking more with the people who have lots of abuse data or maybe using it inside of their products, protecting their customers. But let's take that next step to protect everyone and try and get these harms off the internet. We just integrated a company within the past couple weeks that specializes in phishing as it relates to crypto. And so, boy, I'm seeing an influx of these, like 200 a day phishing domains specifically related to crypto. And it's great because that's just not data that anyone else has. And so it's really fun to be able to see that stuff come offline.

And there's some links and how to contact me at the end of this presentation, but I'll stop there and take questions. Boy, how'd I do on time? Not too bad.

MASON COLE: You did great. Thank you, Graeme. Very good. I'll take a cue. And we have Steve up first. Steve Crocker, please.

STEVE CROCKER: Thank you. And thank you, Graeme. Two things crossed my mind. The first is sort of adjacent or some perhaps tangential, but in the process of accumulating responses from RDRS users who made requests, we encountered a somewhat odd, at least to my thinking, a somewhat odd situation in which some of the people who made requests into RDRS for registration data discovered that instead of getting the registration data, the registrar treated it as an abuse action and took the domain off the air without giving back the details of who was the registrar. And

some of the requests, so it was interesting that some of the registrars viewed giving out registration data was more risky than simply taking down the site and dealing with it that way. So first thing is, do you have any comments or questions or thoughts about that? And then if I can remember what the second point was, I'll come back after you respond to that.

GRAEME BUNTON: So broadly speaking, we have stayed away from access to registrant information at the Institute just because it's been such a landmine within the community and we felt it was often an impediment to getting work done. Re registrars deleting or suspending a domain name rather than passing off the information. I have vague recollections that a registrant might be able to opt to do that. Like there's been a request for your information. But I have no idea if that's actually a thing or true or enabled across the space. I could also see it though that the request for information causes a registrar to go look at it at a registration and be like, "Oh, this does look super sketchy. It's pretty clear that this is fake information in this record. I'm going to go look at what payment they used maybe. Oh, look, that credit card is sketchy." And so they've engaged their own abuse processes. And so I suspect that probably happens a fair amount, but that's based on speculation and not data. Interesting. Very interesting. Thank you.

CRYSTAL ONDO: Hey, Graeme, can I answer to Steve as well? So my best guess here is that when you ask for data, a lot of them are being requested for

phishing reasons. And then people, like Graeme said, registrars look. And the risk of taking down a phishing domain name on a registrar is between the registrar and that customer. And if they're engaged in bad action in terms of service, it's a pretty easy thing to do. Providing PII to a third party based on a request opens a registrar up to liability, not just from that person, but also from any various bodies, political, EU bodies, data protection authorities, about the disclosure of that data. So it's a bigger liability risk actually to give away PII than it is to take down what a registrar deems to be an abusive domain. So I think that's probably where you're seeing a slight disconnect, is that the registrar is balancing their liability risk and going with the lesser of the two.

STEVE CROCKER: It's very interesting. The rest of the conversation belongs in a different form related to requests and so forth. So I'll suspend that. The other thing, Graeme, that was on my mind, do you have any sense of abuse reports that are inappropriate, that are for the wrong reasons and would cause problems as opposed to helping clear things up?

GRAEME BUNTON: I have some sense of that, although I don't have hard numbers. One observation I've got as a sort of related to this is that my impression from many people who report abuse is that they think they are better at it than they are. And that a lot of people who are doing this almost professionally, let's say, or as part of their business, are still not great at it. And I think that is mostly because they have not gotten reasonable feedback or timely feedback or useful feedback from the registrars

they're reporting abuse to. And so I think a lot of the work in this space that needs to be done is about collaborating on standards, getting people to talk the same language about what a useful, actionable abuse report looks like, what to put in it, what's going to get action at a registrar. So there's still, I think, quite a bit of low hanging fruit there.

I see going through NetBeacon, as part of that 23,000 odd abuse reports we saw, there's still some percentage of what I would consider to be a useless abuse report. And I guess as an aside, I think of registrar abuse handling time is zero sum. And so a bad or inactionable abuse report is worse than no abuse report because it's consuming resources that are finite. And so we do still see a percentage that are like, for content related issues that are just not appropriate at a registrar, we see, you know, our forms prevent some real junk from getting through, but just people who are mad about something else and using these forms or these abuse reporting processes for other things, it's still pretty common.

STEVE CROCKER: So that's very helpful. You've made a distinction between sites that are compromised versus sites that were intentionally created. I think that's a very insightful distinction. And so it causes me to wonder about the abuse reports that are inappropriate, whether there's a comparable distinction between ones which are inappropriate because the people well intentioned, but not very good at it, to say, versus ones that are purposefully submitted to cause problems where they shouldn't be submitted at all. Have you thought about all that?

GRAEME BUNTON: A little bit. I will say the places where I've seen most obviously weaponized abuse reports, where people are sending them in to cause trouble, is typically cyber criminals trying to disrupt other cyber criminals. Like it's competition within the bad guys doing bad things. And so that seems to be the mode, like I haven't seen, yeah, I have not personally seen at least in what's going through NetBeacon, weaponized abuse reports I don't think aren't related to cyber criminals trying to disrupt their competition.

MASON COLE: Thank you, Steve, for the question. That's pretty interesting, Graeme, that you have cyber criminals fighting it out on registrar platforms. Who would have anticipated that? Margie, please.

MARGIE MILAM: Hi, this is Margie with Meta. Graeme, thank you so much for the work you guys are doing in this space. It's really important. And I think it'll be interesting to see how the reports change, if you will, or the results change as the new amendments come into place. One of the things I'd be interested in seeing in the reports is tracking of what the registries and registrars do. Because I think some of that you can see through the WHOIS status changes. Obviously, you won't see everything because you won't see, for example, if it gets reported to the hosting provider. But I think that's a very telling statistic, primarily in the area of maliciously registered domain names. Because in that scenario, it doesn't make sense that, at least in my view, that the mitigation should

only be at the hosting level. Because that just invites basically website hopping, right? Jumping from one host to another host. And really, the only way to prevent that would be through action either by the registry or the registrar. So I would encourage you to take a look at that and see whether that's something that can be tracked.

And then the other thing about reports, and this is something I think that the broader community should have start talking about is, let's talk about the definition of DNS abuse. And there may be areas where reports are submitted that a registry or registrar may not feel falls squarely within the definition, but it's a gray area. And I suspect you're probably seeing things like that. And in my view, those are things like imposter domain names, where it's pretty clear that the domain name is being essentially teed up or registered for phishing, malware, fraud, but it actually hasn't happened yet. So an example of that would be something like, you know, Facebook login, you know, Facebook support center. I mean, those are the kinds of things that as a major platform, we see again and again and again, and in trying to, you know, protect the user from harm from that, you know, that's an area where I think, you know, if we could talk about imposter domain names as another threat, you know, angle that should be addressed through the DNS abuse definitions or processes that might do, you know, a fair amount of proactive work that would prevent harm to consumers. So just a thought and would like to hear, you know, your reaction to those concepts.

GRAEME BUNTON: Thank you. And I'll try and be brief, because I don't want to consume your whole meeting. reattribution for mitigation. We do capture that as part of the Compass project in order to measure mitigation rates and time to mitigation, we are capturing in the underlying data, what that mitigation look like. And so that's client hold, server hold, either by the registrar or registry. Often it could be the name servers change, either because the host has done something or maybe it's being sinkholed, or the content has changed. Some of that could genuinely be the bad guy has finished what they're doing, like if they're changing the name servers to something else, or they're, you know, so there's some fuzziness in the attribution outside of client hold and server hold. But that is a thing that we will begin looking at over time and trying to bring forward. But it is complicated work.

Re impostor domains, I think of them as like suspicious domains. So domain that looks sort of on its face, kind of shifty, you know, it's login dash support, dash, you know, famous brand dot tld. I think that's an interesting place for some work. I have a best practice that I wrote on this that everybody hated. Because, you know, trying to encourage registrars to, you know, go look at this in in more depth. But my sense is, I'm not fully all the way there on that best practice. And the community is not all the way there on what to do with those domain names. But it is a potential avenue for more work. But the paper's not out, it's not published. Because it's got some rough edges. I'll stop there. Thanks.

MASON COLE: All right, Graeme. Thank you, Margie. Thanks for the question. We're at 30 minutes past the hour. One last opportunity for questions for Graeme before we cut the queue, please. Okay, Graeme, very good. Thank you for your time. Thank you for your expertise. Appreciate the update to the BC and hope you'll come back and present to us again at another meeting down the road.

GRAEME BUNTON: I'd love to. I really appreciate the opportunity. Thanks, Mason.

MASON COLE: All right. Take care, Graeme. Thanks. All right, friends, we are at 30 minutes past the hour we are at agenda item number three, which is now our policy calendar update. Steve, over to you, please.

STEVE DELBIANCO: Thanks, Mason. I've displayed on screen set this out yesterday. Since our last BC meeting on the 21st of March, we've filed two reports. On the 21st, we filed a report supporting ICANN's plan to reserve .internal strictly for private use, widespread unanimous support in BC. Thanks to Crystal Ondo for drafting, we submitted that. And then on the 2nd of April, two days ago, we submitted our comments on the draft applicant support program. Remember, these are grants to applicants for new gTLDs, grants and technical and financial assistance. And then there's a handbook provided for them. David Snead, with some help from Vivek, prepared. Comments were agreed, whether they had properly implemented the handbook, what some probably would come up with

as a spec. And look, we made very broad comments that said some of this is really complicated. So if we are targeting applicants from demographic communities that aren't very sophisticated, technical, financial in domain names, they're going to have a tough time with the handbook. And I think that was a powerful comment from BC. I want to thank David and Vivek for that work, and Lawrence, who had been on the working group.

All right, scrolling down, and there are several open public comments right now. And there are a few that we need to handle today, because we won't meet again before the comment closes. The first is on the string similarity review guidelines. Now, we have circulated last week a draft, which thanks to Hafiz Farooq, to pull together what the BC would say about the string similarity guidelines. And I think that everything that Hafiz had in the draft is fantastic. But I am trying to call out something that we should go further on. And that is the notion of whether string similarity could include a singular and plural of the same name, dot book, dot books, dot hotel, dot hotels. We were very concerned about that 12 years ago, and I remain concerned. And I know that at least Crystal weighed in on lists this morning to agree.

If you look at the guidebook they've put out for this, ICANN is saying it is a non-goal. They put it in the appendix. They say it's a non-goal. Plurals and similar in certain European languages, the Romance languages, plural terms can be formed by just one little s. And they go on to say it is potentially confusing. But however, because they believe that there are other examples where the plural doesn't require an s, French language, there are some in English where they add it. And then they went on to say is that because it's language specific, they don't think they should

deal with it. I've got to say, if it is a problem in the English language, if it is a problem in some of the Romance languages to simply add an s and it makes it confusingly similar, then ICANN should not be preempted from making that part of the string similarity criteria. Because whenever they're examining a couple of strings, they're often looking at the linguistic community of users and registrants that are targeted by that language. So I'm just so disappointed at the implementation that they've come up with in these guidelines to say that it's not a goal.

So I would propose that we include language, encouraging ICANN to do this and develop guidelines to prevent the delegation of singular plural forms of the very same string where they're confusingly similar when the plural is just adding the letter s. Now, I understand from Crystal that the board shares, some board members share the same concern we have and wondered why the working group didn't come up with this beforehand. And it may be that the board cannot get in the way of something that has already been through the process. But look, this board frequently will come up with ways to weigh in on something that was missed or mishandled by the community. And I think this is one of those instances. But let me ask for a show of hands to comment on. You can comment in the chat. I'd like to know whether there's widespread support in the BC on this because we would need to add that comment before the 10th of April and circulate it to all of you. Margie's a plus one. Anyone else? Marie? Does anyone object to us adding that? All right. Fantastic. I don't see Hafiz on the call today. So, I will put that into the draft and we will circulate another one before Monday. Thank you.

All right. Moving to the next one. There's a proposed bylaws update to limit the use of the accountability mechanisms. What am I talking about

here? Like an independent review panel, a challenge to a board decision, or a challenge for a board non-decision related to some of the things that we accomplished in the transition of the IANA function to give the community the ability to do challenges, but also to allow individuals to file IRPs. That's been around for a while. And the notion here was that the limit the access to one of these accountability mechanisms. And it looks to me as if what ICANN's doing is expanding this amendment beyond just a limitation on those who've received money through an auction. And Margie and Lawrence, I know you volunteered to draft the BC comment, and I'm inviting us to broadly suggest whether or not ICANN is trying to limit its vulnerability to challenges by broadening the idea of things that cannot be challenged or things that you could not challenge if you received any auction proceeds. Have you guys thought about where you're going with this comment and can discuss it with the members? We've got plenty of time to get a draft in their hands, but I wanted to know what you're thinking. Lawrence, Margie?

MARGIE MILAM: This is Margie. Yeah, I've been remiss. I've been behind on my work. So I don't know if Lawrence has had a chance to think about it. What I can do is work on something tomorrow and circulate it by the weekend so we have time to think about it.

STEVE DELBIANCO: That would be outstanding. Just even a draft set of points that we will later refine into sentences. Any adults in the BC following this issue

closely enough to be able to contribute? Anyone in the BC that's been part of an IRP, you would have personal experience on it. Okay, moving to the next one. There's a draft handbook for registry service providers. This wouldn't ordinarily be something the BC would be too concerned with unless it involves criteria for what a registry service provider vendor would need to honor with respect to their ability to handle abuse issues with their financial stability. BC members include registrants and registrants jumped on a new TLD run by a registry service provider only to learn that that registry service provider lacked the financial and technical expertise to withstand a cyber attack or went out of business. Look, the harmed communities in those cases, the harmed communities are the registrants and business registrants are our core constituency. So I don't think it's a surprise that the BC ought to comment on this and fortunately on our last call we had plenty of interest. Vivek Alan, Crystal, John, and Segunfunmi all agreed to work on that. So those comments don't close for about three weeks so you look for some draft to show up prior to our next call. Would any of the drafters like to talk about what you're considering on this and do others on the BC have interest in helping? Segunfunmi, I see you on the line. Have you started looking at this yet?

SEGUNFUNMI OLAJIDE: Yes, I'm looking into it already and it's been a good one.

STEVE DELBIANCO: Okay, look forward to a draft circulated between yourself, me, and the other drafters so we can get something pulled together. Alan, please.

ALAN WOODS: Thank you. Much like Margie, [inaudible] so I had a proper look at it today. But for those of you who haven't looked at it, it's 108 pages long, is this RSP document, so we have a bit of wading through. A lot of it is technical stuff but yeah, hopefully if somebody can, you know, get the pen started on this one, I'd be happy to pile in a bit on that.

STEVE DELBIANCO: And Alan, we can focus only on elements that would be relevant to a registrant who paid the money and printed new business cards to change their TLD only to learn that the ICANN process for RSPs was admitting people that aren't competent or qualified to do it. So we can really narrow our focus and we don't have to comment on elements of the guidebook, the handbook, that aren't relevant to that. Thank you. Appreciate your help on that.

The .XXX registry is proposing dropping their sponsored TLD or STLD designation and move to the generic, the base registry agreement. Now the BC's position on this, we did this on .Museum, is the promises that were made to the registrant and user community, promises that are binding, should be ported over from the sponsored agreement to the spec 11, the public interest commitments if they're going to move to the new agreement. And adopting that new agreement or renewal shouldn't be a way to hide the ball if what they're trying to do is to shed certain obligations. And I did want to point out the .XXX didn't have a lot of content related obligations, but they did have some promises made to entities that they would fund with proceeds from the registry. I don't

even know if that entity's still around to help with it anymore. But we need to develop a BC comment that might well focus on the same things we said about .Museum. And I would invite BC members who would be willing to take a look at this. These are the promises made in a sponsored TLD and whether they should be imported into the spec 11 of an STLD. Can I find any volunteers on this? Seems it's rather legalistic. Unfortunately there's only a handful of promises. They're easy to see when one looks at the red line of the proposed agreement. When we see a red line like this, it indicates that ICANN or legal has already met with and negotiated everything. When they put these comments out for public comment, these revised agreements, there's very rarely any change to it. Margie, I can't believe you're signing up with all the things you're already committed to, but I'll be grateful for your help to look at .XXX. Is there anyone else that would help Margie on this? We can just focus on commitments that are relevant to the safety of registrants. Let's make sure, for instance, that they don't allow them to register the name of your company .XXX, especially if it's easy for them to do a trademark clearinghouse check. Anyone else? Thank you, Margie. And finally, I'll turn to Sven and Marie to talk a little bit about where NIS2 is right now. Marie, you gave us the update in yellow. What would you want us to point out to your colleagues about that?

MARIE PATTULLO: Before we do that, Steve, I see Lawrence is back with his hand up.

MASON COLE: Lawrence, can you get through now?

LAWRENCE OLAWALE-ROBERTS: Great. So, back to the comments that I volunteered for with Margie. My understanding of the ask from ICANN Org is to be able to take certain decisions without having to always come back to the community, especially with regards to the [CCDW] on auction proceeds. What was put out for comment was just an amendment to the bylaw. Basically, they are asking for us to give our support to the amendments or not. This particular issue seems to be of interest to the wider community. It's also something being discussed from the council side and from the comments that have come in from the registry side, the contractor parties, the registries, the registrars, and definitely from the IPC, it appears that the community is wary of giving so much power as it may to ICANN Org to be able to literally take decisions rather than coming back to either the community or the empowered community.

While it doesn't look harmful on the surface, but in terms of being able to hold ICANN accountable for actions, the BC might want to align also with the position that we definitely want to have sufficient mechanisms in the bylaws to be able to deal with issues of this nature that come up. Where there is a particular issue that needs to be addressed that seems to be in conflict with the bylaws, ICANN Org should come back to either empowered community or to certain aspects of the community to seek direction on what to do. That's the line in which I'm thinking that the BC comment might go and would like to be guided because we are also asked for input or for feedback to be able to give counselor direction.

STEVE DELBIANCO: All right, that's very helpful and I will volunteer to help on that as well because what you're getting at is this notion of we created the empowered community in the transition. The empowered community is supposed to approve whenever the ICANN Org wants to change a fundamental bylaw. Some of this board resolution is to avoid having to seek that approval. You realize that in Hamburg we made a relatively minor change to a fundamental bylaw and we had to convene the empowered community. We did it on the last day in Hamburg. It took about a half an hour and I was one who spoke that this was an appropriate exercise of that muscle. ICANN, the community, the empowered community, we can come together quickly, study a proposed amendment and give the required approval by the bylaws. So why would the board and Org try to sidestep a process that we've only used once and had it go smoothly? That would be another story to tell. Appreciate your work on that, Lawrence and Margie. Marie, you want to tell us anything new about NIS2?

MARIE PATTULLO: Sure, very briefly because I'm conscious of time. We understand there is an open consultation now in Sweden but we haven't actually seen the text in anything but Swedish. We'll follow up on that when we can. What you've highlighted is another document that's come out of European Commission. It's not about domain names per se, it's about counterfeiting and piracy in general, but it does have some proposed best practices that include that which is in NIS2. So I'd really encourage you to read it. It's very short. A recommendation in European law terms is a form of law but it's soft law. So it's not binding, it's not mandatory, but it can be for example referred to in court and it is something on

which the Commission intends to follow up in I believe three years to see if anything is happening. Steve?

STEVE DELBIANCO: Marie, will any of the Member States try to implement these recommendations as part of their NIS2 transposition?

MARIE PATTULLO: Well, we hope, so because what it does is if you like it sets out this is the opinion of the European Commission and for example it talks about verification methods to provide for verification procedures for domain name registration data. It also talks about taking voluntary measures to detect incorrect registration data for existing domain names. What to me is very interesting is it also mentions that domain name service providers are encouraged to recognize as legitimate access seekers any natural or legal persons who make a request for a right of information under the European Union's IPR Enforcement Directive. In other words it gives a legal basis for the request for the information which is something as you know we've been continuously told is a barrier.

Whether the member states will do so, Steve, no one can reply to, but it is very important that this is the Commission's perspective.

MASON COLE: All right, thank you Marie. We have hands up from Steve Crocker and then Margie please.

STEVE CROCKER: Thank you. Thank you very much for this. You started by suggesting that we should read this and comment on it. Would somebody, either you or somebody else, be so kind as to circulate this to make it easy for us to access it or at least give us a pointer to it? Thank you.

MARIE PATTULLO: Absolutely, Steve. The link is already in the policy calendar that you see there. If it doesn't work let me know and I'll send it to you again. For the purposes of comment, this document is now published. We commented on it a lot of times during its drafting which took about three years. So the document is already out there. It is already a done deal. But as I say, if you can't click on the link, if it's not working, tell Steve and he'll let me know.

STEVE CROCKER: All right. I just tested the link and that is working. So you ought to be able to get right to that page. Margie.

MARGIE MILAM: Hi everyone. Yeah, I took a look at this document and it's really helpful in terms of clarifying the legal basis for getting WHOIS information when you're doing an IP lookup or trying to get data to protect your intellectual property. The reason why I think it's useful is because I think many of you remember at the ICANN meeting there was this notion that, oh, there's no right to get the data. And what the paper actually does is it walks through another directive. And I don't know, Marie, if

you can elaborate on that one. I hadn't really followed that as closely before.

But it basically says when you're trying to protect your intellectual property, you have the right to request the data. So it actually recognizes that and I think clarifies some of the issues that we were dealing with years ago in the EPDP when we weren't sure how the legal basis would apply in the area of intellectual property. And it also has a provision related to trusted notifiers, I believe, some sort of trusted notifier concept. So all of those are great things that we should be talking about as we get ready for the next ICANN meeting and as we have continued discussions with the board about updating the current WHOIS policy, especially where these clarifications help shape why there should be reveals on WHOIS information when it's related to intellectual property. So just wanted to flag that and think about how we can elaborate on that as we, you know, get ready for the next ICANN meeting.

STEVE DELBIANCO: Thanks, Margie. We'll jump quickly to council. There hasn't been a council meeting since our last BC meeting on March 21. Lawrence, do you have anything to add? I put in your expected items to be on the agenda for the next council meeting on the 18th. Go ahead. Anything to add? If not, we'll just move on. Okay.

The next up would be council activities. And I want to give Zak and Arinola an opportunity to seek BC members' input because by tomorrow, they'd like to have our thinking on the transfer policy

changes. So what I have in here is a summary of what Zak circulated last week on the 28th of March. That information is to seek feedback from us because Zak and Arinola will be putting in the BC's position. And they've already drafted their position and I attached it to the transfer policy feedback. Zak, I'll turn it to you to see if there's any pointed questions you want to put to BC members right now.

ZAK MUSCOVITCH: Thanks, Steve. Well, as Steve mentioned, I'd sent out the draft policy recommendations last Thursday and requested feedback from BC members. And as Steve also mentioned, I'd like to get that feedback in tomorrow so there's time to submit it before next Tuesday's meeting. Can I get a sense of who intends to provide any feedback at this point in time so I know whether we don't have any or whether we can expect some? If anyone cares to raise their hand or put it into chat or mention it verbally?

CHRIS LEWIS-EVANS: I'll be putting in some feedback by tomorrow.

ZAK MUSCOVITCH: Okay. Terrific. Thank you so much. Anybody else? Okay. Well, it's not as sexy as DNS abuse, but we'll work with what we have. I'll also mention that I was in touch with the IPC's rep, Mike Rodenbaugh, the other day and shared with him the draft feedback that I had prepared and sent to the BC members, as mentioned previously. And his sense was that that's the same position that the IPC should take. And so he asked if he could

share that with the IPC. And I said, well, sure, but let me just wait to see what feedback we get from the BC on today's call. So, Chris, if you have any feedback, if you're able by any chance to shoot it to me sooner rather than later, so I can try to coordinate with IPC as early as possible. Thank you.

STEVE DELBIANCO: Zak, Rec 17 is something we would support. And you're worried that Jim Galvin's objection will lead the working group, give them an excuse to reconsider the recommendation. So we would encourage you to be strong in trying to preserve Rec 17 approach, despite Jim Galvin's concerns.

ZAK MUSCOVITCH: Thank you. And I'll also mention for what it's worth, my sense from at least one registrar representative is that they're in favor of that Rec 17 too. And so they intend to keep, well, they're not pushing for it, but I expect some support to come from them. There may be some tweaks to the proposal that I'm trying to work out beforehand, but thank you for that, Steve. Appreciate it.

STEVE DELBIANCO: Thank you, Zak and Arinola, appreciate that. Steve Crocker, anything you want to add on RDRS? Just a couple of notes in there.

STEVE CROCKER: No, the exercise which you and the IPC made a very, very strong and important contribution of hosting that session, that report is that we put together and attempting to summarize, but not supplant the

transcript, is now out. I think, I'm not sure whether it's completely published, but it went through all of the extra review that was sort of added on at the late—So it's taken a couple of weeks, which I did not have in mind. So I think the question is, how do you guys feel about the fact that you hosted this? Some of the registrars felt that it put them in a bad light or that it wasn't appropriate. I'll have to say from my point of view, I thought the whole thing was a smashing success, both in content and in process in the sense that it made the point that channel four, the reg requesters was an important part of the overall system and that having it controlled by either staff or the contracted parties was not the entirely appropriate way for things to be done. And I thought the registrars should have thought that this was really good feedback on their behalf, as opposed to feeling aggrieved by it. But that's just my opinion.

STEVE DELBIANCO: I share your opinion, 100%. To suggest that we said things that should have given offense, especially in the hard edged environment of ICANN, is amazing. We took great care. We took great care to avoid being pejorative in the discussion.

STEVE CROCKER: So that's all I have to say on this. I thought it was, as I say, very helpful and raises the question of whether you want to do it again or maybe not immediately at the next meeting or some other time. But I do think that having the people who are requesting the data, having a strong voice and being viewed as at least co-equal to the people who have the

data is a very important point to make and that you should not be at all hesitant to be just as forceful next time.

STEVE DELBIANCO: Yeah, and I have a feeling we should do another one in Kigali if we can. That's what I would suggest. All right, thank you. All right, I'll turn to channel three, which is the CSG. Marie, I have all of your notes pasted in here. Anything else you want to talk about?

MARIE PATTULLO: No, everything's there. But to stress, if anybody has experience with the problems we've had to date in nominating our board seat member, our board seat, sorry, board seat 14, our board member, and feels happy to share them with me that I can use in the ongoing negotiations, please let me know. Please have a look at the very basic scoping document that is attached to the policy calendar. Thank you.

STEVE DELBIANCO: Thank you, Marie. Questions for Marie? Oh, great. So I get to turn it back over to Mason with one minute left.

MASON COLE: Good job, Steve. Thank you. All right, we made it just under the wire. Any questions or follow-up for Steve DelBianco, please? All right, then we are at the end of our agenda, skipping item number four due to Tim's absence. Brenda, I believe our next meeting is 18 April, correct? Yep, you have it on the screen. Okay. All right, very good. Thank you,

Brenda. Any other business for the BC today, please? All right, everybody, we have some work to do. Thanks again for all the volunteering and pitching in. And thank you, Brenda, for the support. And straight up on time at the top of the hour, we'll talk to you in two weeks. The BC is adjourned. Thanks, everybody.

[END OF TRANSCRIPTION]