BRENDA BREWER: Good day, everyone. Welcome to the Business Constituency Membership Call on the 8th of April 2021 at 15:00 UTC. This call is recorded, and attendance will be taken from the Zoom participation. Kindly state your name before speaking, and have your phones and microphones on mute when not speaking.

And I'll turn the call over to Mason Cole. Thank you.

MASON COLE: Thank you, Brenda. Good morning, good afternoon, good evening, everyone. Mason Cole here, chair of the BC. Welcome to the BC Members Call on April 8th 2021.

The agenda, Brenda has put up on the screen for you. You can tell that it's a bit different this morning. We have a guest with us who's going to occupy the first half of our meeting. And then we'll move to the regular part of our agenda. Just fair warning. We may run over a big today because we've got so much to cover, but we have an opportunity to interact with Graeme Bunton who's the inaugural director of the DNS Abuse Institute. And he's asked for a place in our agenda today, which we've accommodated.

And Graeme is going to lead a discussion on what the DNS Abuse Institute is all about and how we can cooperate. And I encourage everyone to have a very interactive discussion with Graeme because he's prepared to have one with us.

Before I turn it over to Graeme, are there any changes or additions to the agenda? All right, very good.

Graeme, welcome to the BC call. Thank you for joining us.

GRAEME BUNTON: Thank you for having me, Mason. I really appreciate the opportunity to talk with you guys today.

MASON COLE: Well, good. Thank you. It's good to have you here. You have a good section of our agenda today, so I'm going to turn the floor right over to you. And I encourage you to make room for questions and interaction along the way if you don't mind. The floor is yours.

GRAEME BUNTON: Great, thank you. Yeah. My intent with this is to be as bidirectional as possible. I've done a fair bit of unidirectional speaking at people so far, and almost something like a road show I'm doing about the announcement of the institute. And so, the more that I can get feedback and interaction and new ideas and more information, the better. So, don't be shy, I guess, would be my recommendation for today's chat. So, let's go to the next slide, please. Thank you, Brenda.

In recognition, 30 minutes of your hour-long call is a good chunk, so I really, again, appreciate that time. A gentle apology to people who have seen a little bit of this before. I've done some introduction to the institute in a couple of places, and I know some of you are engaged in

those other places as well. So, please bear with me. I'll try and say some new things in there, too.

But what we're going to do today is that I'm going to introduce the institute for a bit. I really do want to hear from the BC and members of the BC to gather some input and ideas. And that is towards making sure that I'm communicating with the community, and that as I'm building the roadmap for the institute and what we're going to try and get done, that I've got some really diverse perspectives and that I'm meeting some goals that satisfy a broad community of people.

And then the last piece is going to make sure that you guys have my contact information. Feel free to contact me and we can make sure that there are some open lines of communication there. So, that's what we're going to try and do in the next 25 minutes or so now. If I could go to the next slide, please. Great.

Why? The "why" here is really why did we create the DNS Abuse Institute. And I should say the "we" is really PIR. Public Interest Registry who run .org established the institute and approached me—I guess I still applied, some combination of those two things—about running the institute and getting it off the ground.

And the "why" is relatively straightforward. DNS abuse has clearly been a conversation of importance within the ICANN and broader Internet community for at least a couple years now. I think if you look beneath the surface, it's been a topic of concern for even longer than that. It's just that we've had other things in front of it.

And so, there has not been some real concerted, concentrated action in the issue. We've sort of left it within the individual registries and registrars to try and deal with, and there are some gaps there. And PIR was seeing those gaps and looked at their public interest mission and decided that they had the resources and capability to try and do something about this.

So, here we are. There's an institute. I'm in charge. And maybe for those who don't know me, because there are people on this call that I don't know, I spent the past 10 years working for a registrar call Tucows, a large wholesale registrar. It was the second-biggest. I think now the third with the amalgamation of Web.com and Endurance. Somehow, I don't work there anymore. It still stings a bit.

I spent four years as chair of the Registrar Stakeholder Group. I spent a lot of time working on DNS abuse in that capacity; started the Registrars DNS Abuse Working Group within that structure. I tried to get some movement there.

And one of the things that I experienced in that role was really that ICANN has a particular role within this space with regards to DNS abuse, but it's really bounded by contracts. Individual registries and registrars have things they care about, but the industry is generally—at least on the registrar side—high volume, low margin, very competitive.

And registrars are not very good at collaborating, which might be a surprise to some people here who see the Registrar Stakeholder Group as a particular structure. But the industry as a whole does not play well

together. And that really impacts the ability of the industry to come together that touch us all like DNS abuse.

And so, I could really see issues where we had no one dedicated to pick up the pen and do some work or really coordinate best practices across the industry. And so, that was frustrating me and I didn't have time to do it in my previous job either. So, with the opportunity to lead the DNS Abuse Institute, I really began to tackle these things in a concentrated manner, provide the resources to the community. It was really exciting to me.

So that's, I guess, what I'm talking about in this slide [that] there's no organization with a mandate to really tackle this issue. There are structural impediments within the community to really coordinating on this issue. And so, here we are with it—this brand-new institute.

And I should say it comes out, to a certain extent, of that Framework to Address Abuse that a number of contracted parties have signed and I helped co-create when I was back at Tucows. And PIR was a key piece of that, as well. And so, it was a really natural fit, I think, for PIR to set this up.

I should also add here, and I think this is important to note, and I'm sort of hearing some quiet, backchannel questions, let's call it, about the relationship between the institute and PIR, how that sits within the ICANN community. And I guess what I want to stress is A) what a great thing PIR has done, but B) I am definitely legally affiliated with the registry. But I want the community to feel like there is some daylight between the institute and PIR as a registry.

I'm not looking at all at PIR's abuse processes, at the complaints that come in to PIR. I'm really not looking at the registry business at all. I'm really focused outwardly on the community as a whole and what the institute can do. And over time, I think we may, we'll see, greater independence for the institute from PIR. That's certainly TBD.

But I don't want it … And it would be a problem for me—I guess I would say, if I'm being very frank—that people see the institute as just an extension of PIR or an extension of a registry protecting registry interests.

That's not what I signed up to do. That's not what I'm here to do. I'm here to make the Internet safer and better, and I'm not necessarily … And I'm definitely not here just to protect a particular registry.

So here, a complicated thing which is that I'm deeply appreciative of PIR. I think there's no one else in the space better situated to step up and do this. But, also, see me as independent. If you can hold those two things at the same time, please do so.

And certainly, as I'm trying to get this thing up and running, not having to go around with my hat out to try and get other people to contribute to stand this thing up, is great. That would be consuming 80% of my time as opposed to really trying to make a difference on DNS abuse. Next slide, please.

And I'm not paying attention to hands, but if you want to throw up your hands, I'll try and keep an eye on that.

So, the institute has three pillars that we've settled on to try and drive our agenda forward. Education is going to be a key one. And that is really ensuring that we have freely-available, robust resources for registries and registrars on different types of DNS abuse, best practices on tackling DNS abuse—the bits and pieces they need to do the work.

But then also, educational resources for people who are reporting abuse: intellectual property, law enforcement, Internet security, etc. And there are some real gaps there. And in fact, I had a great conversation with some people from RIPE NCC—actually, not from the organization itself; from the RIPE community—[who has a] numbering piece on their anti-abuse side. And they had all of these same problems that we do on the naming side. And that was really interesting to me.

And so, I think there are wonderful opportunities to collaborate, which is the next pillar. Which is really to contribute to discussions, bring these different parties together. And that includes people like yourselves—registries and registrars, the hosting industry, the numbering community—to really figure out where we can collaborate and get people together.

I see a hand from Mason. Please, go ahead.

MASON COLE: Thanks, Graeme. I don't mean to interrupt the presentation, but I just wanted to bring up a question on the education front. So, resources for abuse reporters like IP and LEA, registrars and registries—it seems like, often, we speak different languages when it comes to abuse. Does the institute have a plan for harmonizing that language in some way so that

when we talk about abuse, we're speaking about the same numbers and we're speaking the same language, etc.?

GRAEME BUNTON: Yeah. Good question, Mason. "Plan," I think, is maybe a little bit stronger than where we are at the moment. So, I have a roadmap, and I'll come to that in a slide or two. But on the common language front, I think a lot of that education gets to best practices and standards and evidence that should hopefully get people sort of coalescing.

I still think there are a lot of conversations around definitional issues, and I'll talk about that again in a minute. So, maybe, let's come back to that question at the end of this intro and see if I've left some gaps that I can try and fill, if you don't mind.

So, I've just sort of done education. Collaboration. Innovation is this last piece, and this is the one that really got me the most excited to join the institute. This is where we need to fund research to really understand DNS abuse. But it's also really about building tools, like actually things that people can use to address DNS abuse. And I'll talk about what those look like in a sec.

But I should mention here that all of this is free. This is not a commercial endeavor. There are no fees for any of this. All of this is meant to be part of the public interest mission. So, PIR is well-funded. They've got great resources. We can go and spend some of that to make these tools happen, and that's super interesting to me. So, let's go to the next slide, please.

MASON COLE: Graeme, you've got a hand from Mark there, please.

GRAEME BUNTON: Hey, Mark. Go ahead.

MARK DATYSGELD: Thank you for having you, Graeme. This is sort of a continuation of a conversation we started on another call, but I would like to bring it to the broader BC membership. We are very interested in this generation of resources. Right? We are pretty excited about exactly this concept of generating research and producing high quality material in different fronts. What I'm interested in knowing is how interested is the institute in working together with partners in this. For example, say the BC decides to develop a resource on DNS abuse.

Is this something that the institute would be willing to promote if it finds agreeable, for example? Or provide us with support in the sense of data, help us connect with different actors. How do you envision that the institutes grow in relation to the production of materials, be it educational or attempting to gather facts and so on?

GRAEME BUNTON: Thanks, Mark. So, I think as part of my roadmap, I've got a lot of work to do on building the institute's capacity to understand DNS abuse. And that is going to be a really key deliverable for me. I think we need to have the best-in-the-world intelligence on DNS abuse. And so, that's

going to mean, for the institute, coming up with pretty clear definitions if we're going to measure stuff, robust reporting that's accessible to the community. It's got to be transparent so that people can understand how it's built and replicate it if they see fit.

All of that work, I think, we will invite community input on before we commence that work. If I'm being quite frank, I think we need to hold the pen a lot as we're getting started and building capacity within the institute. I think relying too much on or a lot on broader community efforts might end up diluting our work a little bit or slowing us down.

Ultimately, I think that collaboration pillar of the institute means that we need to be really accepting input and willing to work with input from the rest of the community that's concerned with DNS abuse. So, I want to make sure that people have the opportunity to contribute. Where there are resources from the community that are useful and good and drive the conversation forward and help reduce DNS abuse, I've got to be crazy to turn those down and not bring them inside or help promote them.

I guess I would like to be community agnostic, and so it doesn't matter if it comes from the BC or the IPC or outside the ICANN world at all. If it is relative to the mission of the DNS Abuse Institute and it is useful for reducing DNS abuse, I think I'm obligated, in a sense, to take that on board and see what we can do with it.

MARK DATYSGELD: Thank you very much.

GRAEME BUNTON: Next slide. How far are we in? We're about 15 minutes in? Great, okay.

Initial focus is really what I'm thinking about as I'm building at the roadmap for the institute. And so, this is really how can I reduce DNS abuse? What's the biggest impact I can have with the least amount of implementation?

And I say implementation in a specific way, having spent 10 years working for a registrar, and 4 of those in charge of essentially that entire industry—insofar as one can say that's true. I've seen registrar development backlogs. So, any work that requires a registrar or even a registry to go write code to mitigate DNS abuse, I think is a real problem.

And those backlogs are filled with projects that either generate new revenue or to keep, frankly, gigantic aging registrar platforms—because most of them were written in the early 2000s—up and running. And so, trying to get them to do work, write code, I think just means that these projects take years and years.

What I really want to do, or at least the first focus for me is going to be getting tools into the hands of the frontline compliance people. Can I get them better information in a more timely fashion and reduce the amount of work they need to verify those abuse reports to really streamline those activities?

And one of the points on this that came you in our first webinar we did a couple weeks ago was that GoDaddy was saying that they receive

something like 2,000 reports of phishing a day. But the vast majority of those were either duplicates, or not actionable because they had no evidence, or just were wrong.

And so, if I can reduce that load of complaints from 2,000—and I don't know the figure exactly, but let's say—of which 1,500 were not useful to just to 500, boy, I free up an awful lot of time for a registrar to go do meaningful work on abuse. And I think that's really important.

So, I'm really not focused on integration. I'm really focused on those frontline abuse people. At least to start. I think that's where we go in the first couple of years. I really need to build the institute's capacity, so that's really understanding the tools. That's block lists, for example. And I think I was alluding to this earlier, was really standardized reporting on DNS abuse.

And so, to that, I think this will be interesting for people here. And again, I don't have my roadmap approved by either my advisory council or anyone else yet, so still working on that.

DAAR exists, the Domain Abuse Activity Reporting system that ICANN created. It's now a few years old. It has some weaknesses. I think people don't find it particularly transparent, and it's constrained by what ICANN thinks it can or can't do. I have a really strong feeling that in order to be authoritative on DNS abuse, we can't rely on third parties to say what's happening and we need to build our own DNS abuse intelligence system.

I think the key pieces for that are that we need to be able to talk about what individual registries and registrars are doing. We need to do it for

CCs as well as Gs. And we need to talk about persistence rather than existence. So, if someone's being really active in reducing DNS abuse, we want to make sure that we're able to reflect that.

And we also need to only be reporting against abuse that's actionable. Is it evidenced abuse reports? Because if it's just a domain and there's nothing else with it, a registrar can't typically do anything with that.

So, that's sort of my initial focus. I can see some stuff in the chat. Trusted flaggers. Reducing resources on both sides. This is a topic that comes up quite a bit, the trust notifiers. And I think I made this point to Mark relatively recently in another forum as well. That trust is really … You can't impose that on any particular party. It's got to be bidirectional so that the registry or registrar who's going to be taking action has a deliberate choice in that.

But what I can do, and what I think we can do is make that easier. And the way I think we do that—and this is going to be one of the key things I'm going to be working on or would like to work on—is a centralized abuse-reporting tool, again, on a roadmap that no one else but me has really seen or approved yet. So, all of this, these plans with a grain of salt. And, again, there will be opportunities for community engagement on these plans.

But if I can build a place that is one place on the Internet. You plunk in the domain name, it figures out which registrar that's with, you tell me what type of abuse it is, and it requests the specific evidence for that specific abuse. And then you can submit that. It just goes to the right registrar.

That A) solves some of this abuse-reporting problem that we've got where we're able to generate really quality abuse reports that are actionable. But B) it also allows people submitting abuse reports to develop a reputation, to be able to say, "I've submitted 1,000 abuse complaints. 100% of them were actionable and correct and good in some fashion."

Now, you have some real hard evidence to say, "I'm a trusted reporter." And that allows you to take that to contracted parties and say, "Hey, can we smooth this relationship over a bit?"

So, I think there's a big opportunity there. That particular idea of the centralized abuse-reporting system, I think people have thought, "ICANN should have done this a long time ago. It doesn't feel like they're going to …" And so, that's the thing I would really like to begin working on. Next slide, please.

And I'm losing track of the chat here, so if someone has something they wish to raise, maybe stick up your hand.

Right. The definition conversation. This comes up quite a bit in just about every discussion on DNS abuse that I've ever had with people outside of contracted parties. The Abuse Institute has adopted the definition, same from the Contracted Parties House, "Malware, pharming, phishing, botnets, and spam where it's a vehicle for others."

We are going to be hosting another forum—"we" being the institute—likely in the second week of May. We're still sort of locking down the details of this. My argument here is that if you're … And I was making this argument on our first forum. If you're to graph a distribution of DNS

abuse, it's a normal curve. There's a huge lump in the middle that is 80% stock-standard DNS abuse. We don't need to argue about the definition. Everybody understands what it is. And we need to do some work on that core problem. And I think that's really where the institute is focused.

I think there are interesting discussions to be had about the margins, those definitional discussions. They're kind of fun to have. The overlap between content issues and DNS abuse where the most obvious example is phishing and intellectual property issues. What does that overlap look like? I think we can have some discussions here, but really I'm focused on that 80% in the middle problem.

Do I have more to mutter on that? I have some strong opinions on the way to do this. One of the things I think we're going to do on this next forum is really to step through examples, to have as most concrete a discussion as we can have on what abuse actually looks like and how we move away from core DNS abuse to what I would then call content abuse. And just to really discuss where people see that shifting.

I guess I will say, having worked at a registrar for the most part, I think—we use the phrase good actor/bad actor—the people engaged on DNS abuse like this definition because it's actionable for them. These are concrete things that they can understand, that they are comprehendible to a registry or registrar. And so, that's where they feel comfortable acting. It's typically not out of laziness or a desire to not do work.

But I also understand that opportunities for resolution of online harms on the Internet are rare. Hosting is entirely unregulated. And it's really

difficult to find other places other than the DNS to resolve a bunch of problems. And so, expanding that definition can be useful.

I think we'll continue to have conversations on this definitional piece probably for forever. But I guess I just really want people to hear that if we can make some real difference on that big problem in the middle that's causing real harm to millions of people and we can show some progress on that, that gives us a bit more room to discuss those margins. And that's really where I want to make sure I'm focused, in the middle. Next slide, please.

MASON COLE: Graeme, just a quick five-minute warning.

GRAEME BUNTON: Great, thank you. Right. Delightful. So, this is—and there's lots going on in the chat. And again, [sir], I'm talking too much to follow, but as you heard a little bit about the institute, do you think I've … I haven't displayed the whole roadmap. I will publish that soon, but I would love to hear from you guys about where you would spend your time if you were me. And as you guys are concerned about DNS abuse, what are the tools you wish you had?

And I see a hand from Susan. Susan, please.

SUSAN KAWAGUCHI: Hi. Can you hear me?

GRAEME BUNTON: Yep.

SUSAN KAWAGUCHI: Okay, good. You just never know. So, I was wondering. One thing I'm seeing when we submit on behalf of customers to the signatories, enforcement notices, we do submit to every player in the ecosystem. It could be hosting, registrar, registry. So, I can understand the confusion sometimes in the duplicates, but why is a duplicate an issue? If GoDaddy is getting 10 notices for one domain, that seems like that's more validation.

And then let's say they're only getting two, so that cuts their numbers in half. I can understand if they're not getting the information they need, but if you look at your framework there's no real instructions and guidance on what we need to submit. Because if we had that … There is some language and things, but if we had that, then we would follow that where we could.

And I asked that questions during the ICANN meeting and got a variety of response and some things that didn't seem feasible. So, if that was something you could … Do you always need a screenshot? What is it that you need? And then that would make the reports well founded for those that have to research them and say okay.

But the reality is that large companies trying to combat this are going to use several vendors: a phishing vendor, an enforcement vendor—maybe their lawyer, too, because it's whack-a-mole. But we'd be happy to know that we could streamline this and could offer a solution that would get more results.

The other part is, when we send those notices on behalf of customers, we don't get a standard response. Which is fine for part of this, but if I send a notice in to a specific registrar to [say], "Hey, we have no information due to GDPR. We're sending this to abuse@registrarx," I will oftentimes get the same auto response as I do to sending a notice with naming the signatory.

And it just seems like just a good practice that the signatory of the framework would have a notice that is specific to that so that you have some belief that, okay, this is not going their regular abuse process. That it's getting some special notice within their systems and that they'll take action.

GRAEME BUNTON: I think I just cut you off, and I apologize if I have. I recognize that we're probably going a little bit long in time and I want to make sure that if anybody else has questions, they can get in. But I'll see if I can answer that quickly.

The standards for evidence piece is a thing we clearly need to work on. Registrars have a document on their website—I know this because I helped write it—about the evidence required for particular submissions. But that's really not uniform across the industry, and so this is where I think a centralized reporting tool can be helpful.

And the more that I can work to standardize that across contracted parties and say, "Hey, this is how you should do it," the better. Standardized responses are interesting, and that sort of comes out of the work of [that] Internet and Jurisdiction project where I think they've

done some work on that. And I need to think about how we would implement that.

On the multiple reports and why it's a problem for registrars and registries to get 10 abuse reports on the same thing, it's partly a tooling problem. It's still another ticket in a queue that someone still has to go and look at. It's not like your Zendesk automatically collapses those into one place. And so, there is a real … Someone's still got to look at it 10 different times.

The other is that the original source of that abuse complaint might be the same block list, and so there's nothing new in those 10 different things, and trying to treat them all as an increased evidence doesn't make sense. It's the same things from 10 different places, but they all came from the same RBL. And so, I don't think that strengthens your case in any meaningful way, and that's a problem. We need to figure out …

And a thing I'm thinking about is really understanding the various sources for DNS abuse as they come in, which ones are evidenced, which ones are the best quality, have the lowest false positives; and how to ensure that registries and registrars get that information in a timely fashion in a single place. A lot of this requires centralization in an interesting way, and I need to think about whether that's a good idea and how to execute on that.

SUSAN KAWAGUCHI: I've got a couple more things if I can, and then I'll be quick.

GRAEME BUNTON: I'll leave that up to Mason, maybe, because I recognize that we're now almost 40 minutes into your call.

MASON COLE: Thanks, Graeme. Susan, go ahead and then we'll cut the queue from there. And Graeme, there have been some other things raised in the chat that might be useful to you. I'm going to ask Brenda, if she can, to save the chat up to this point, and we'll share that with you so that you can follow up on anything in there that's valuable.

GRAEME BUNTON: Great. Brenda, if you could just go one more slide ahead, too, please. And thank you. It's just so that people see my contact information and a head shot. You're welcome. All right, sorry. Susan, go ahead.

SUSAN KAWAGUCHI: Okay. And thanks for the extra time, Mason. So, traditionally we've always seen some for the ccTLD registries take proactive actions on new registrations, and we are also now seeing—in the last year, at least, is when I realized it—that some of the new gTLD registries are doing that.

So, Radix, for example. If they see a domain name with a famous brand and login that is a typo—or not a typo, but most of the brands are forced to register brand login for protection—they will suspend that domain and investigate it. So, they proactively take a stance that there are certain terms and certain brands, probably. It's got to be a large,

well-known brand. They're protecting their own registry and not allowing those to be used. So, they usually are put on server hold or the name servers are removed.

And so, I was wondering if that is something that the registries that are signed onto the framework, are they considering taking other action and just get those easy ones? And I completely understand that phishing is not based on using a domain name with a brand in it. It can be done without anything relevant in the domain name. But if you get rid of the easy targets, it just seems like it's one more step in the right direction of making this harder and less relevant for the phishers.

GRAEME BUNTON: So, I think this comes back to a point I was making earlier where … I agree there are some very sensible things that contracted parties—I try and say registries and registrars because I really do want to approach CCs as well, I'm not just focused on the ICANN community—that they could do proactively on registration.

So, is someone registering something with a -com in the domain name? You find that it's pretty frequent in phishing. Does that elevate the registrant verification process? Is someone registering more than 15 domains at a time? Okay, now maybe they don't resolve right away and there are increased verification processes there. You've got to call or something like that.

Can you do machine learning models that are looking at new registrations and comparing them to DNS abuse and flagging potentially problematic things? There are lots there. Those are potentially really

good solutions, and I think some of them are very sensible. But those, to me, are further down the road for the institute to work on just because I'm aware of how much work it is to get those things built across an industry.

And so, I think that would take years to get on backlogs and get developed and implemented, and I think there's a lot more we can do with providing better tools, resources, and best practices ahead of time.

So, those are good ideas. We'll capture them. We'll encourage them. But it's not, I don't think, going to be the focus of the institute.

MASON COLE: Okay. Graeme, thanks. I don't mean to interrupt, but I think we need to cut the queue right there because we're six minutes over time now. So, are there any closing thoughts that you might have that you'd like to share.

GRAEME BUNTON: No. I just really appreciate the opportunity and the discussion. My job is to ensure that we're doing this collaboration and working with the community. I really encourage people to pay attention to the upcoming webinar when we announce that. When we announce our roadmap, which will be public, to really dig in and provide feedback on that. And just send me an e-mail, reach out, find me on Twitter. The more ideas I can get, the more I can hear about people's pain point, the better. So, don't be shy.

MASON COLE: Thank you. We'd like to have you back at some point later in the year when things are up and running and have another conversation if you're willing.

GRAEME BUNTON: Absolutely.

MASON COLE: Great. Graeme, thanks for joining us today. I really appreciate you coming to talk to the BC.

GRAEME BUNTON: Thank you. Take care, all.

MASON COLE: All right. Take care. All right, ladies and gentlemen. We are slightly behind time today, and I'm just going to reiterate that we're very likely to go overtime slightly. So, apologies for that.

Let's move straight into agenda item #3. Steve DelBianco is on the call today, so I will turn the policy discussion over to him. Steve. Steve, I think you may be muted. Having a hard time hearing Steve.

All right. Brenda, can we—

BRENDA BREWER: Steve, your phone line ... I'm sorry to interrupt, Mason.

MASON COLE: No, please.

BRENDA BREWER: Steve, it's your phone line that's muted.

STEVE DELBIANCO: Can you hear me now? I just decided to bag the phone line.

MASON COLE: There you go.

BRENDA BREWER: Okay. Yes, we do. Thank you.

STEVE DELBIANCO: Okay. It wasn't [muted]. Hey, thanks, everybody. Mason, I'm going to see if I can get us back on schedule. Okay?

MASON COLE: Great.

STEVE DELBIANCO: So, rapid fire here. So, since our last meeting, we commented on EPDP Phase 2 Policy Recommendations. A really hard-hitting letter that stayed out of the weeds but had a pretty powerful comment. I know

that the contracted parties on EPDP were pretty alarmed with the BC letter. And then just the other day, Monday, we commented on a couple of aspects of the .us registry's plan to allow privacy in proxy services.

So, let me turn to the open public comments. We have two. The SSR—which is Security, Stability and Resiliency—their Review Team Final Report closes today. And Jimson, many thanks to you for the initial draft, and to Denise Michel who contributed a lot of the details. Now, the attachment for today's policy calendar includes edits that were made by Mason Cole yesterday before the deadline. And they really do clean up the comment and make it flow more sensibly.

So Jimson, as the primary author, we'd love to have you take a quick look at what Mason put in. And I'll file it at the end of the day today. Are there any comments you want to make about that, Mason? Or other members who have questions for Mason?

MASON COLE: I don't think so, Steve. It should be self-explanatory.

STEVE DELBIANCO: Anyone else? Thank you. And then we have another comment which is not due until the 14th of April, and it's on the initial report of the ccNSO PDP on how they're going to retire Country Code Top-Level Domains that are obsolete. Now, we have Jimson and Lawrence who have volunteered.

Lawrence, I'm looking for you to draft something very brief. An e-mail is probably sufficient. And we want to get that out by tomorrow so that members have a full seven days to review.

LAWRENCE OLAWALE-ROBERTS: Okay. I'll work on sending something out for tomorrow.

STEVE DELBIANCO: Great. Thanks, Lawrence. In the list there, I indicate the previous comment we did about a year ago in July of 2020 which you worked on as well.

Okay. Mason, [we can turn] to the next one. On Tuesday, we had a call with Contracted Party House leadership focusing on DNS abuse. Since some of that is a little bit redundant to what Graeme just went through, I'll leave it to you, Mason, as to how much you want to report from that Tuesday call. It's on the screen in front of us.

MASON COLE: Thanks, Steve. Actually, it was with more than CPH leadership. It was about five or six BC members, too—about 20-25 Contracted Party House members.

The Contracted Party House under the registries and registrars have an internal working group on DNS abuse, and they posed a number of questions to us, kind of like Graeme did just now. What are your pain points? Where do you see areas of cooperation, etc.?

We had a one-hour conversation which was, I would characterize as, fairly fruitful although we really only got through the first, probably, question and a third. And it seems pretty obvious to me that if we're going to have an ongoing dialogue with the Contracted Party House, which I believe we should, that we're going to have to reconvene and have some discussions.

I find, personally, that we're still at odds with Contracted Party House over things like definitions and what really constitutes abuse and what contracted parties should be obligated to talk about or to do about DNS abuse.

So, I would characterize this as early stages of discussion with the contracted parties and something that we need to continue. I think that should sum it up, Steve.

STEVE DELBIANCO: Mason, what I put in the policy calendar was the definition they've suggested. And that was embraced by Graeme today. And underneath it, I just reiterated for argument's sake a far, far broader definition from about 11 years ago. Now, when I brought that up on that call Tuesday, boy, plenty of pushback from contracted parties across the Board. Really don't want to see anything like the second definition, this one here that's on the screen in front of you all.

So, if you wish, tactically I can beat that drum to see if it provides any movement. But I strongly doubt that it will, and I would recommend that we really take advantage of things like what Graeme is working on.

Let's work on tools. Let's work on specifics and not get tangled up in a definition that's going to be hard to change.

Now having said that, there are elements of, let's say, copyright infringement and trademark infringement that is designed to fool customers of legitimate businesses. When that happens, that feels to me like it's fraud. But they would love to categorize it as phishing, pharming, or spam as opposed to saying that it's an intellectual property concern.

So, one of the things we have to work out is whether we're satisfied with their framework definition. Or do we have to fight to change it? Any thoughts on that, Mason or others?

MASON COLE: I agree with you 100%, Steve.

STEVE DELBIANCO: Well, look. Not seeing any hands up, so I will move on. The next item which is the modification through policies [in] GDPRs, all pushed to the bottom of the policy calendar. Just yesterday, we had a call that Ben Wallis arranged with Ben, Mason, and I. And it was a 35- or 40-minute call with the European Commission [to connect] to walk through our suggested clarifications. Now, Ben Wallis is going to reprise that after I finish running through the policy calendar, so I'll save that for later.

Let me turn now to Mark Datysgeld and Marie on GNSO Council. You'll see that I've recounted the meeting on the 24th and what was passed,

and then I go on to talk about your meeting on the 8th. And I don't have any information on your meeting on the 22nd yet. Marie and Mark.

MARIE PATTULLO: Hi, Steve. Can you hear me?

STEVE DELBIANCO: Perfectly.

MARIE PATTULLO: Okay, thank you. We have an extraordinary meeting later this evening. What fun. And it's going to concentrate on four things, and there are three of them that I think are very important to us.

Now, the first. It's some of the stuff that came out of the Phase 1 of EPDP. But the most important part is an old friend proxy and privacy, PPSIA. Now, the question that we've been asked to look at is given … There are commonalities between Phase 1 and the PPSIA where recommendations are similar or overlap.

Can the EPDP recommendations supersede the PPSIA has part of harmonizing the two so long as the intent is maintained? Now, I have a big concern about that. I've already pinged an e-mail to some of you because this is pretty much the same wording that was used when we saw the death of thick WHOIS. Unless you tell Mark and I differently, my assumption is that we still believe that there's quite a lot of PPSIA that can be put into effect right now. And it should be unpaused.

There are clearly parts that may be affected by EPDP, but not that many. So, unless you tell me differently, that's the way we're going to go. Okay.

The next is accuracy, our old friend accuracy where, again, there is a whole discussion paper which boils down to me being worried that they're trying to delay everything. I can't imagine why I'd be worried about that. But they are suggesting using some ICANN Board terminology that there should be some kind of a study first. So, although we've got the scoping group already, there should be a study, in essence, to look at what we're trying to measure.

I'm also worried about some wording that strikes me that what they're trying to do is say that this is all about whether or not GDPR and other privacy legislation had an effect on accuracy. Now, what concerns me there is that the answer is, "No, it didn't, because it was inaccurate before and it's inaccurate now." Okay, good. Move along.

This is not, to me, what we should be looking for. I believe that the scoping group should be about—God forbid—having accurate data and figuring out a way to get there.

Now, I'm really so grateful we have Susan and Alex on that scoping team. And calling you out, Susan, I sent you an e-mail just before this call with the briefing paper I just referred to. I'd be really grateful if you would have time to cast your eyes over that and give Mark and I a couple of pointers before later.

And the final one I want to bring to your attention is that we're going to be talking about the SSAC's comment on the SubPro report. Now, the

standout to me of the SSAC comments—I'll quote it—"The SSAC recommends that the Board, prior to launching the next round, commissions a study of the causes of, responses to, and best practices for the mitigation of the domain name abuse that proliferates in the new gTLDs from the 2012 round. This activity should be done in conjunction with implementing the CCT Review Team's relevant recommendations."

Now, that goes an awful lot further than the discussion we just had with Graeme. What we're going to talk about in Council is, is Council going to react to this and how? But I think that is a fascinating statement from SSAC.

And I will now stop talking and hand over to my wonderful co-councilor, Mark. Susan, it is at 19:00 UTC, and I will put the link the chat. Thanks.

MARK DATYSGELD: Thank you, Marie, for covering pretty much everything that's relevant. So, I will take the opportunity to very quickly compliment what we were discussing with Graeme. I'm growing more and more convinced that the problem with DNS abuse from the contracted parties side is not philosophical. It's not anything. They just don't want to spend the money on it. Period.

I've had maybe, I don't know, six meetings about this—bilateral to multilateral, whatever. And it all comes down to that. They don't want to spend the money. Okay, how can we help that? Right? We're obviously not going to funnel money to them. We already do. Don't we? But at the same time, there's a gap. Right?

There's an opportunity there, and I am seriously looking into how to address that. And if anybody wants to brainstorm together with me. Some of you already are. But if anybody is not involved in this but would like to be, make sure to reach out. I'm still looking at what we can do at the Council level, but at the same time, we …

As a constituency, we have a lot of members who could conceivably help fund and help move this along. I happen to be a researcher specialized in ICANN, as some of you know. A lot of you guys are extra experts in things that are incredibly relevant. It seems like we have the pieces in place to do something instead of just having endless discussions. So, yeah, I'm looking into that. And please reach out. I'll make sure to keep you guys updated.

MASON COLE: Thank you, Mark. Appreciate that. Next up, Waudo. Let's see if we can do a brief report on CSG liaison.

WAUDO SIGANGA: Thank you, Steve. I think I'll be very quick because since the last BC meeting, only two activities have happened with the CSG. The CSG has actually been in some kind of recess. The first activity that happened after the last BC meeting was that the CSG held the open meeting at the ICANN70 and a few issues were raised there.

Maybe I'll just quickly mention a few that I think that … The BC, we had a meeting with Göran Marby, the CEO for ICANN. And some of the

topics that were discussed there included Internet governance where the BC fielded some questions that affect the BC, for example.

The BC was interested in the difference between technical Internet governance and the policy work that we are doing just to make sure that we are on the right path as we are doing that work. And Göran replied that ICANN has tow distinct branches, the policy making process, and also has a technical mandate. He gave some examples of running the root server relationship with IETF and so on and so forth.

He also mentioned that there is a fuzzy intersection between the technical Internet governance and the policy making. But he mentioned that that should inspire more engagement between the two divides.

He also had an interesting suggestion to form what he called an intersection group bringing together ICANN Org and all components of the community in their interactions. So, I think that is something that we could think about going forward.

There was an item about ICANN meetings. He mentioned that after the survey that was taken after ICANN69 on the meetings, we can expect quite a number of changes. And then he also said that the meetings should be about people coming together including in groups outside the usual ICANN meeting.

He mentioned that opening up of the face-to-face meetings has to take into consideration that recovery from the pandemic might not be evenly distributed across the globe. So, if we are thinking of involving everybody in the meetings, we may have to consider that some parts of

the globe might not have recovered from the pandemic while some other parts might have recovered.

There was a topic on compliance which of interest to the BC. The BC has been calling for an enhanced role for ICANN compliance in DNS abuse. And Göran replied that the ICANN compliance is the place to test if implementation of the policy has worked. So, in sort, he kind of pushed the thing back to the policy making within the GNSO.

Then within that meeting, also, we had a session with Mr. Ajay Data, the chairman of the Universal Acceptance Steering Group for Universal Acceptance.

Then just quickly, the next meeting that we are going to have is a CSG meeting with GNSO-appointed Board members. This is a follow up to an earlier meeting that we held before ICANN. And we are looking for topics, so if members of the BC have some topics that they would like to be discussed there, we'll accept those. Although the ones we are thinking about right now are continuation of the ATRT3 Holist Review, things like … They were talking about the bylaws and the next steps.

We're also going to continue talking about DNS abuse which, as you can see, is very important for the BC as well as the PICs enforceability. So, a formal invite, I think, is going to be sent out by Brenda to the BC. And as usual, you'll be invited to attend the meeting and also to contribute to the agenda items. Thank you, Steve.

STEVE DELBIANCO: Thank you very much, Waudo. Appreciate that. Ben Wallis, I'm going to quickly display the comment we filed on NIS 2 and give you an opportunity, then, to talk through the call we had with those individuals yesterday.

BEN WALLIS: Thank you, Steve. So, we filed comments to the European Commission's consultation, and separately we've sent some views directly to legislators. The European Commission contacted us and requested an informal meeting to discuss this response to the Commission consultation that Steve is showing on the screen. And we had this call yesterday.

Now, in many ways, the BC comments are about seeking clarification or more detail in the provisions to ensure that they capture all of the right actors and achieve the desired outcomes. So, we're generally very welcoming that Article 23 exists, and we just think it could be clearer and more explicit in a number of ways to make sure it does achieve those desired outcomes.

Now, it was of some comfort, therefore, that the Commission's intentions in drafting the article were fairly well aligned with all of these clarifications that the BC wanted to see. They intended the same things that we're asking for. And in some areas they did concede, but it might be helpful to clarify their intention. But in a lot of ways, they didn't see it as helpful or probable, or even desirable, to do this within the articles of the directive as we're suggesting.

They also explained that it was a conventional approach within European law to avoid too much detail and prescription, and instead that the article should state the principles and the desired results but leave space for the member [states] and those actors subject to the law to decide how they will achieve those aims consistent with those principles.

So, there was some comfort there. I don't know if we have time to run through their response to each of the five areas of comments that we have, but I think it's definitely worth reconvening a meeting of the drafting team to think about the detailed feedback they provided and to think about whether that merits some kind of reconsideration of our strategy and of what we're asking for.

The legislative process is still at an early stage, and there's plenty of time for us to refine our asks and hone in on specific amendments and prioritize. So, I don't think it's something we need to do urgently, but I think it would certainly merit the drafting team getting back together and thinking about it.

The Commission also had a few suggestions for what we could do that would be helpful with regard to NIS 2. They said it's important to show how Article 23 contributes to cybersecurity, and they've received some criticism that it's not sufficiently cybersecurity-focused. It's about much broader issues, and this directive is specifically about cybersecurity. And, indeed, in our position paper for the legislators, we've provided only examples related to how WHOIS data serves the interest of cybersecurity.

They were interested in us talking about how WHOIS data can be useful for data protection itself and for demonstrating how Article 23 is not in contract with the ICANN process, but rather is there to help the ICANN process work.

And finally, they suggest that we think carefully about picking certain battles, [kind of] noting that we've got quite wide-ranging asks here for changes to the Directive.

So, Steve, is that enough for now or did you want me to go into any more detail?

STEVE DELBIANCO: No, I think that's fantastic, Ben. And thank you, again, for leading our effort on this. Now, many BC members would probably appreciate a written evaluation from you on the reaction we had. But let's be sensitive to confidentiality concerns that some of the members of the European Commission may have.

So, what are your thoughts about circulating a written explanation to BC private, or would you prefer to just do it during a phone call?

BEN WALLIS: I think in terms of the entire Business Constituency, if there's a desire to understand more details, it might be better to set aside some time to do that verbally during the next BC call. And that if I do share this detailed written summary, it may be best just to do that within the drafting team. And given, as you say, that the European Commission emphasized

that this was an informal call, I think they are sensitive to keeping things off the record to a certain extent.

STEVE DELBIANCO: Thank you, Ben. Are there any question for Ben, or do we turn this back over to Mason? Thank you, Ben. Mason, all yours.

MASON COLE: Thank you, Steve. Thank you, Ben. Brenda, if we could have the agenda, please. All right. While Brenda's putting that up, I believe the next item on the agenda is a quick report—here we go—from Lawrence on Operations & Finance. Lawrence, over to you, please.

LAWRENCE OLAWALE-ROBERTS: Can you hear me okay?

MASON COLE: Yes. If you speak up, we can hear you well.

LAWRENCE OLAWALE-ROBERTS: Okay. I'll try and speak louder so that I'm more audible. So, to start the report, based on time, there is an open ICANN community announcement for the chair of the GNSO Policy Development Process for the working group on the Review of Transfer Policy. This closes next week, the 16th of April, and this is an opportunity to serve and it might be of interest to some BC members.

We currently do not have any new member to report, but we're currently in the process of producing some customized BC outreach materials, and they will be available for download and review once the design and concepts are all ready.

Currently, we have finally evolved our transition to the new BC URL, [icannbc.org]. And we will also be maintaining our former site at bizconst.org side by side this. We have some customized e-mails where you can reach BC officers, and this has been shared on the mailing list. The details will also be in my [thoughts] that I will share with members much later.

In the coming meeting, or subsequently, we will be unveiling a new BC logo, and we want to ask members to look forward to that.

The BC FY22 Draft Budget Proposal and the financial report for the current financial year will be made available on the BC private list for members to review and comment. But just to say that our finances have remained stable, as they were. We currently have close to $60,000 as a closing balance because we are maintaining our reserve fund. But there is set apart in the [general], $60,000. So, our finances are healthy.

The BC committees. We have an ongoing call for volunteers for the BC committees. This has been shared on the private list, and we expect that, from today, members interested in serving on the Communications and the ICANN Learn and on the boarding committees will indicate their interest. A few members have indicated interest before. We appreciate your stepping up on this. We encourage more of us to step up to this opportunity.

In the same vein, we are also seeking volunteers for the BC DNS Abuse Working Group that was [noted] on the last call. We're expecting subject matter experts to please step forward to help form a formidable team with regards to pushing our interests in terms of DNS abuse.

There is going to be a candidate call at our next meeting on the 22nd of April which is Thursday, and it's going to be 30 minutes earlier than the scheduled members call. So, aside from those of us who are volunteering, we want to encourage members to be available for that call.

For the DNS Abuse Working Group and the [recommendations] working party were constituted. Both groups are not bound by our election [rule] because it's open with flexible membership. Wherever there is a need to refresh the membership of the DNS Abuse Working Group or any of the recommendation working parties, the BC membership will be made known of such a need. But for the committees, we'll definitely be standing for election if more than the required number of persons indicate interest.

So, if we have more than seven people for Communications, there will be an election from the 22nd running out … From the 26th running out to the 30th of April. And if we have more than five persons indicating interest for the Onboarding committee, then we will have elections also [staged] for those.

That will be all for me at this point. If you have any questions, I'll be willing to take them. Otherwise, I'll yield the floor back to the chair.

MASON COLE: Thank you, Lawrence. Any questions for Lawrence? Okay. I've had a number of people either in the chat or on e-mail let me know that you're interested in joining the working group on DNS abuse. Thank you for that. I'll collect that and Lawrence and I will coordinate on getting the working group up and running. All right, Lawrence. Thank you for that report.

We're doing pretty well on time even though we're a bit over for the day. So, before we close the meeting, let me ask for any other business. Any other business for the BC today? All right, very good.

Ladies and gentlemen, thank you for indulging us on going over time today. It was a very fruitful discussion with Graeme, and I think we had a good meeting. So, if there is any follow up, feel free to contact me offline. Otherwise, the BC is adjourned for the day. Our next meeting is April 22nd. And please be aware, as Lawrence just mentioned, that we will start that meeting half an hour early.

All right? Thanks, everyone. BC is adjourned.

[END OF TRANSCRIPT]