JULIE BISLAND: Good morning, good afternoon, good evening, everyone, and welcome to the DNS Abuse Mitigation PDP1 Working Group call taking place on Tuesday, 07 April 2026. We did receive apologies from Dennis Tan, and the alternate assigned is Chris Dispain with the RySG. Statements of interest must be kept up to date. Please raise your hand or speak up now if you have an update to share to your SOI.

All right, seeing no hands. If you need assistance updating your SOI, please email the GNSO Secretariat. All members, participants, and alternates will be promoted to panelists. Observers will remain as an attendee and will have access to view chat only. All documentation and information can be found on the DNS Abuse PDP1 Working Group wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name before speaking for the recording.

As a reminder, participation in ICANN, including this session, is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct. And with that, I will turn it back over to you, Paul. Thank you.

PAUL MCGRADY: Great. Thank you, Julie. Let's jump in. We have a lot to do today. Our agenda is welcome. That is what we are doing now. Next up will be an update on the meetings and schedules, meeting schedules and holidays, a quick update on work plan, and board liaison. Then we will do a quick wrap on question one, and then we will continue on our discussions of two and three.

So let's go ahead and do that. We have a decision on the schedule and holidays. You guys saw the list of things that will be pushed over to Tuesday for certain holidays through the year. Good exercise. The whole point of this is to lock in our schedule and make it super predictable. We do not want to lose ground making these decisions ad hoc. As you guys can see, it takes quite a bit of time. To do that repeatedly through the year, it would be a mess. So we are locked in. Show up, and if you can't show up, send your alternate, and we are going to move along. Anyway, this is the absolute last chance for anybody to scream. If not, we will lock it in.

I see no hands for anybody, so that is great. Locked in. Next up, updates on work plan and board liaison. Jen, I want to know, would you like to jump in here, or I am happy to give the update.

JENNIFER CHUNG: You can go ahead, Paul. This is Jen.

PAUL MCGRADY: All right. The work plan has been submitted to the Council by our liaison, Jen Chung. Council will take a look at that, and assuming they agree with us, they will approve that, and then that also will be locked in. Thank you all for finding nooks and crannies to speed the work. I will say that I am reading and hearing everybody who also has raised concerns about quality, that we can't move so fast that we don't do a good job. Totally get that. I do think that this is a wonderful aggressive timeline and I fully expect that we will meet it. But I also hear those who are resisting further decisions to speed the timeline at this early stage.

We may well beat this timeline. We just don't know. In any event, thank you for all those who contributed to this discussion. We will go on ahead.

I didn't mean to give super short shrift to the cadence and holidays. There is a slide on that. You guys should grab that just so you know, but staff is getting calendar invites out, so that will make it really simple. The work plan will be presented to Council on their 16 April meeting, and I think it just will be acknowledged, and that is that.

Onto board liaisons. We have our board liaisons appointed. Again, Jen, jump in here if you would like to do that. Our primary is Jim Galvin, good guy, knows the space, and so we are excited about that. His alternate for when he can't make the calls is Chris Buckridge. So that is the board's team that will be joining us. Jen, any commentary, anything else on that? Okey-dokey. Great. Perfect.

So we are in our sessions of charter question one, coming to the end of those. Let's talk about sort of where things seem to be landing. From the early input themes, the proposed threshold for triggering an investigation rests with actionable evidence of DNS abuse under 3.18 of the RAA. The GAC input suggested to expand the trigger to a domain name likely to be used in DNS abuse or that has been used in the past but is no longer actively abusive. While the IPC emphasizes that the actionable evidence can come from anyone, the NCSG and registrars' input suggest to narrow the trigger to clear evidence of systematic abuse. Ultimately, the convergence seems to rest on the trigger being confirmed and actioned by DNS abuse under 3.18.

I know that there are those who proposed to expand it, as we just talked about, and those who suggested to narrow it. I didn't see convergence on either in these calls or on that list for that kind of approach. But there was, as far as I can tell, universal agreement that the actionable evidence standard of 3.18 is acceptable to everybody. I guess I will just sort of do this the most direct way I can think of, which is raise your hand if you think that if a registrar has actionable evidence of DNS abuse under 3.18 that they should not undertake the associated domain names check. All right, I am not seeing hands up. So I think that is where we landed. Oh, I see Volker. Volker, go ahead.

VOLKER GREIMANN: Yeah, and just qualifying that, I don't think it should not be... I just think it should not be the sole indication, but that is the only qualification I had. Otherwise, I agree. Thank you.

PAUL MCGRADY: Thanks, Volker. To be clear, there is nothing that would prevent a registrar from being more diligent than that, right? This is just a standard that ultimately ICANN compliance can advise around, and sort of it is the ceiling, not the floor. So thank you, Volker, for that. It is an important point. Seeing no other hands, I think we have well and truly talked charter question number one to death. There were some good things coming out of that that I think have more to do with charter question number three in terms of the scope, reasonableness of an investigation and those kinds of things, and staff has been diligently capturing those.

This takes us to a straw person for preliminary recommendation number one. Let me just give it a read and talk through the rationale, and then we can have a quick queue on this, and then let's get back into two and three. Preliminary recommendation number one: When a registrar has actionable evidence that a registered name is being used for DNS abuse and has taken appropriate mitigation actions under Section 3.18.2 of the Registrar Accreditation Agreement, the registrar must perform an associated domain check. The rationale for that is the working group considered several options that generally aligned on actionable evidence and action taken on a domain name under 3.18.2 of the RAA as the proper trigger.

This trigger is based upon a contractually enforceable requirement, which better ensures that it is unambiguous and verifiable. The trigger also avoids potentially onerous demands on registrar, which could arise from an overly broad or speculative trigger, such as relying on an unsubstantiated report of DNS abuse or prediction of future abuse behavior. The requirements under 3.18.2 of the RAA do not establish limitations, this is to Volker's point, on where the actionable evidence is acquired, which is important. Well, actually, this is, I think, Marc's point, not Volker's, which is important for some members of the working group. What this means in the practical sense is that the registrar can identify the actionable evidence through its own analysis, or the registrar can be informed by a report from any external reporter, for example, law enforcement, cybersecurity professionals, ICANN org, etc. Both are equally valid under the RAA. All right. So taking a look at the straw person, I see I have three hands up. So we will go Reg, Gabriel, and Farzi. Reg, go ahead.

REG LEVY: Thanks. Reg Levy from Tucows in the Registrar Stakeholder Group. I feel like "has actionable evidence" is way too broad. "Has reviewed" and/or "has already taken action" are more appropriate because sometimes people send us things and we technically have that evidence, but they likely didn't send it to the right place so that the right people have that information. I sent some numbers around to the email list that kind of defines the scope of the problem. So just having it is not sufficient. We have to have actually reviewed it and confirmed that the evidence is actionable. I would prefer that we've already taken the action because that feels like a good trigger. We've reviewed it, we've taken action, and now we're gonna do something. But I will leave that as well.

PAUL MCGRADY: Thanks, Reg. Gabriel, go ahead.

GABRIEL ANDREWS: Unmuting for the first time. Just want to make sure you can hear me. Okay, perfect. This is Gabriel Andrews of SSAC. I wanted to flag that there is a timeline introduced here which won't always make sense. If you introduce the text, "Has taken appropriate mitigation actions," that seems to imply that that mitigative action would always occur before you check to see if there's additional domains to take mitigative action on.

In practice, there are going to be occasions in which you want to take your first overt action against all the domains that are associated with

the scheme simultaneously, rather than to say that you have to take action and potentially notify your bad actors of the fact that they're being caught before you check the other domains. So I would caution that that particular introduction of timeline is probably a little bit too far.

But also as a first reaction to Reg's comment, I wonder if there could be text that might be more along the lines of "if the registrar is aware of actionable evidence," something to that extent, because I take her points too. But I do not think that we can support the requirement that action has already been taken for the reasons I just described. Over.

PAUL MCGRADY: Okay. Thanks, Gabriel. Reg, can you get yourself back in the queue? I'd love to have you sort of react to those two concepts, if you don't mind that. Sorry to call on you. Farzi, go ahead.

FARZANEH BADII: Hi, Paul. So we just want to reiterate what we said on the mailing list. Basically, if there is only one domain name that is abusive, we have warned against guilt by association so many times, and we don't believe that having just one domain name as abusive should justify doing ADC. In our justification for our trigger, we need to be proportional as well. I understand that some people argue that there are no human rights impact. First of all, when we talk about human rights, we talk about human rights risk. There could be low risk, there could be high risk.

And also it's not only a matter of human rights, it's also a matter of promoting a culture of surveillance. So we have to be very careful when we want to trigger the ADC. That is why we need to be narrow and all the things that we said on the mailing list. I don't know how we are going to work on this recommendation further, but we have made the suggestion. If we don't like that suggestion, we are open to alternatives that could kind of distance us from just looking at quantitative indicator of one domain name and look at a host of issues that we can ask the registrar to take action on. Thank you.

PAUL MCGRADY: Thanks, Farzi. All right, we have Brian Cimbolic. Brian, then Marc.

BRIAN CIMBOLIC: Thanks very much, Paul. Just a couple responses, reactions here. And apologies, I'm in the car, otherwise I would come onto video. So on the "has actionable evidence" standard, I like that drafting in particular because it mirrors the obligations in 3.18.2 currently. So when does a registrar have to take action on a phishing domain, for example? It has to take action on a phishing domain currently when it, quote, "has actionable evidence." So I like the idea of not introducing a new but related but slightly different standard where we can avoid it.

I will also note too that in my view of actionable, part of... and I understand Reg's point. The determination of actionability, I think, is built into the contract. So a registrar's determination of actionability kind of, in my mind, occurs when it, within a reasonable timeframe,

assesses the evidence anyway. So I actually sort of think that that language implicitly deals with one of Reg's concerns, I would think.

To Farzaneh's point, I just want to point out the fact pattern that we're talking about, and I think Farzaneh would be right, in my understanding, if we were talking about compromised sites. But we're not. We're only... we're explicitly and only dealing with malicious registrations. So I think we should think about the fact pattern here. If a registrar has in its customer account sixty domain names and one of those domain names is IRSsecurelogin-gov.tld, and someone's trying to phish for IRS credentials or whatever, that person, the registrant in that domain name, is ultimately a phisher. They have a certified confirmable case of malicious DNS abuse.

So I think it kind of... I'm scratching my head to see where the real concern would be at looking at the other fifty-nine domains. You have if me, Brian Cimbolic, is the registrant of that domain, I think all of us would agree that it's worth looking at those other domains where you have someone that has clearly engaged in DNS abuse for a malicious purpose, not a compromised case. It's not guilt by association. You are already the person you're dealing with is a phisher. So I'm having a real hard time coming up with a scenario in my mind in which there would be human rights impacted by looking at a phisher's other domains.

PAUL MCGRADY: Thank you, Brian. So I'm going to throw in a concept to sort of smush these two things together and see if it helps. What if it read, "When a registrar has actionable evidence that a registered name is being used

for DNS abuse, which requires appropriate mitigation action?" So in other words, maybe that mitigation action hasn't occurred yet to the point that you may not want to take down one immediately and tip your hand that you know about the bad guy. You may want to take them down in one big whatever. I don't pretend to understand fully all the different strategies that registrars have when they look at these kinds of situations. There may be some things that, because of the nature of the content, you may not want to take down one by itself.

So what if we said it that way? Would that make the timeline make more sense, keep more optionality open to the registrar about the mitigation actions that they are going to take, but still has a baked-in timeline that moves forward? So anyway, it's just an idea. And we have Marc, and then Volker, and then Reg. Reg, thanks for getting back in the queue.

MARC TRACHTENBERG: Well, I don't love that idea only because I think every... where there's actionable evidence, it requires appropriate mitigation every time. It's not when appropriate mitigation action is required. That's the standard in the RAA. But I guess to go to my actual comments, I definitely agree with Brian on this. I think the standard in the RAA is "when a registrar has actionable evidence," not when the registrar has reviewed it. I mean, I think that's kind of implicit, and also, that gives registrars time to wait to not review the evidence to not take action. But we already have the standard, right? So let's go with the standard that we have, and that should be the standard here.

I also don't think the trigger should be after mitigation because that's like putting the cart before the horse. I mean, the mitigation, which is appropriate, might be driven by what other abusive domain names are identified by the registrar when they're doing their ADC. I also, with Brian on Farzi's comments, can't see here how there's guilt by association. Again, these are malicious domain names, domain names that are intentionally registered for DNS abuse, not compromised domain names, right? Someone didn't penetrate the person's account and took over one of the domain names. So there's no guilt by association because it's the same person or party that is controlling these. That's what the associated domains are.

And as far as the human rights impact, I'm not denigrating human rights in any way, and human rights are important, but we can't let some speculative phantom human rights impact, which is completely undefined, obstruct the purpose of the PDP, which is to identify abusive domain names efficiently. If someone can identify what this human rights impact is, we can discuss it, and we should. But to just speculatively throw out as a blocking agent the potential human rights impact, I don't think is fair or reasonable. And if we're going to do that, that just jams up the entire PDP, and there's no purpose of having it.

PAUL MCGRADY: All right. Thanks, Marc. Volker, go ahead.

VOLKER GREIMANN: Yes. Thank you, Paul, and my previous speakers. I think I agree with Marc and Gabe when it comes to the timeliness and the timing of the

review, simply because of operational reasons. It doesn't make sense to look at the same account twice in the course of an investigation. So I would prefer there to be an alternative that also allows it during the review. I absolutely appreciate those comments, and they reflect what we already do, and the language that we employ here should do that as well.

To Brian's comment that when we look at a customer account that has one phishing domain, it means automatically that that one is a phisher, I would like to question that assumption. Because in many cases, we see customers that have one phishing domain that do not have other phishing domains, and that is not just malicious domain names. And sometimes it's resellers of resellers that provide white glove services for their customers; basically, they take care of all registrar notifications and therefore have their email addresses as part of the service. One of their customers might be a bad guy, the other one might not be, but the data that they give to us is the same for both registrations because of a privacy service that they provide that is not immediately recognizable as one. And that has to be taken into account as part of our investigation as well and part of our associated domains check.

Final comment, and just because I raised this before, I'm not going to go into details. I still think that the threshold for the ADC is slightly too low. There has to be more than just one domain name that we are going to take action or have taken action on. There has to be some indication that there's more that makes our check worthwhile. Otherwise, we'll be spending a lot of time checking and not a lot of time actioning, and that would be a waste. Thank you.

PAUL MCGRADY: Thanks, Volker. Before you leave this scene, how does one know that there are more domain names without checking for more domain names? That is what I am having a hard time wrapping my head around.

VOLKER GREIMANN: I don't always know, but there are certain indicators that will make me check. Some of them are based on experience, some of them are based on the type of report that we receive. And if we have the time, I'd love to go into detail, otherwise, I'd provide it by email to just not take time from the live discussions. But I think that's a very good question, and I think the answer that I will provide on that will be able to give a little bit more background. And I think it's best provided by email so we can continue the discussion. Or if you want me...

PAUL MCGRADY: I think... Yeah. Thanks, Volker. I guess that would be a good exercise, but I don't know how to bake in a standard into a contract that says, "in accordance with Volker's experience," right? And so we do need some objective...

VOLKER GREIMANN: I'll give you a couple of examples maybe. I can give you a couple of examples. One, and that's the most common one, is a reporter reports two domain names. When there's two, there's probably more. The other is naming conventions that are being used. For example, while it's not DNS abuse, just as an illustrative example, if it's a phishing domain.

If it says "certain bank minus city.tld," that's a pattern that kind of suggests that there may be more already.

So if the domain naming pattern suggests that this is a part of a series of domain names that has been registered, that's an indication. If it's a numbered domain name, that's an indication. There is a lot of different secret sauce indications that we use to determine whether it was worthwhile looking for additional domain names. And another one is if it's with a particular reseller that we know accepts Bitcoin, that is an indication to look for more for that registrant. There are a lot of different ones that basically make me already suspicious that an ADC will be successful, and in those cases, they usually are, and then it's time well spent. Thank you.

PAUL MCGRADY: Thanks, Volker. Those are all good real-world points. The concern I think is that if everybody were good actors and doing those things, we wouldn't be here, right? How do we build something that applies to all registrars? And again, this goes back to any policy that lists those things will be outdated the next day because bad guys will think of something new, right?

And so I think having the catalog of things that might make someone like you aware that there's more out there, it's useful. But we have to bridge the gap between useful guidance and a contractual requirement, right? So let's do some thinking about that. Reg, go ahead.

REG LEVY: Thanks, and just a reminder to everyone that this is my requested response to Gabe from a bit ago, which I did drop into the chat as well. Gabe indicated that there are sometimes we want to take action against multiple domains at once, and my response to that is, well, how do we know that there's multiple domains before we check? And so, not sure what order that should be going in. But I also wanted to highlight what Lawrence put into the chat, that we should not be further inconvenienced where we aren't going to be mitigating DNS abuse. That the registrar is already doing all of this review and work, and at some point, the returns are going to be diminishing. So we want to make sure that we're riding the right line there.

PAUL MCGRADY: Thanks, Reg. All right. And by the way, yes, thank you for jumping in at my request. It does not count against any perceived or real or not limits. So feel free to come back to us, Reg, with anything. Michaela, go ahead.

MICHAELA SHAPIRO: Thank you so much. Michaela Shapiro, NCSG. This has been a really useful conversation already. I just wanted to comment on a few points, both to Volker's point of these kind of indicators that are there and the point of perhaps needing to update the ICANN advisory based on those indicators. I think that's a really helpful suggestion, though I recognize that it might be slightly out of the scope of today's discussion.

But thinking about the particular recommendation here, I and the NCSG are particularly nervous about this being a very low threshold. Correct me if I'm wrong, folks, on this, but my understanding is, okay, you have

actual evidence it's been used for DNS abuse. You've done something about it under the accreditation agreement. But that means there's a whole host... that seems like a very sensitive threshold, right? That is an a lot of work both to look into all of those. It's more or less one instance, one case, and now we're going to do a check every single time.

So my sense is that's both a lot of work, and it might also be counterproductive to what we're trying to do here to address the issue at hand. Granted, I do agree with a much earlier point that Brian had made about using the standard that already exists in the contract. I completely agree that reference to Section 3.18.2 is very helpful.

And there was a point about putting the cart before the horse when it comes to the ADC needing to come first. My sense, again, happy to be corrected, is that you can take an initial mitigation action. It might... maybe it doesn't cover the full scope of the issue before you do an ADC. That doesn't preclude you from then escalating the response in proportion once the ADC has taken place, right? So you've now found that you do need to escalate the response based on the findings of the check.

So I don't necessarily see that as an issue from my view, but again, very happy to hear what others say. And yeah, just wanted to agree with also Volker's point that just one phisher may not necessarily... they may not necessarily have more phishing domains, and that is a concern that Farzi raised as well on the guilt by association, that presumption there. So just wanted to add those thoughts and, yeah, very happy to hear from others. Thanks.

PAUL MCGRADY: Thanks, Michaela. And everybody, sorry about that noise. My other phone, I did not turn off the ringer. That was on me. Michaela, thank you for that. I think that I see some notes in the chat that I think are helpful as well, especially Tomas and trying to find language to bridge the gap on the timeline on this, I think, is important. We have Eberhard, Gabriel, Brian, and yeah, and more to follow.

EBERHARD LISSE: Okay. I assume that is me then. Eberhard Lisse for the record.na. I have a little bit of concern if we say we must check before... we must do an ADC before we have taken action on the initial complaint. That goes awfully deep into content, which I am very much opposed to. We have already a standard. I am not saying the numbers. It's one or more.

And I think the preliminary recommendation duplicates... the point is it's not so much the actionable evidence. It's if a registrar has taken action against a registrant, then he must check whether it's one domain or two or three. That is not my question. We don't need to put in the actionable evidence because the trigger must be, in my view, that the registrar has taken action. In other words, there was a report. They have found it was true. They have taken action, and then they must go and check the others. So that's the workflow that I would think.

Whether it's a large amount of workload, I don't mind. I don't know whether it can be offloaded to software is another thing. I'm not sure that... That is why I asked Reg what it would cost to do an ADC on one domain. If it can be automated, and I think much of this can, it's not a

problem. But if a human has to sit there, then you have to pay somebody to do it, and that increases the cost enormously, and we should take this into consideration when we make a policy.

PAUL MCGRADY: Thank you, Eberhard. All right, we have Gabriel, Brian, and then Matt.

GABRIEL ANDREWS: Hi, all. This is Gabriel Andrews. And I wanted to respond. I don't recall if this was a direct question or not with regards to circumstances in which registrations occur where you will not know. And Paul, I think you were speaking to this point. You will not know necessarily that there are additional domains. I recall situations where I was investigating bad actors that were engaged in business email compromise scams. This is the kind of phishing where someone will impersonate a CEO. They'll send phishing messages to entice a CFO to send wire transfers to bank accounts of their choosing.

And the bad guys were registering homoglyph domains, lookalike domains, where each individual domain represented a different victim. And I don't know that you would have any indication of how many potential victims the bad guys were registering without just taking the simple action of looking at the account in question and seeing how many domains do they have. And that sort of check is pretty low-hanging fruit.

If you see that this account has two dozen domains, as I recall in one specific circumstance I was looking at, and each of those domains

represented a different victim homoglyph, that could be really important action to take because you're potentially preventing harm to those additional twenty-three potential victims, even when a single victim's homoglyph domain was reported.

And I think that's really the benefit of this policy that we're contemplating, is the ability to protect additional victims against harm by the same bad actor that's using malicious registrations to conduct a scheme against multiple victims. So I just don't want to lose sight of that. But Volker, I do very much appreciate your comments that you aren't trying to introduce extra work. But I do think that we can potentially assuage this by returning to Brian's suggestion from last week.

NEHA NAIR: The trigger to at least contemplate additional associated domain checks is very low and consistent; that there is actionable evidence that there is malicious registration that has occurred. But then the actual check that you conduct should have flexibility, as Brian had suggested last time. That there be more flexibility to do only those associated domain checks with the information that is reasonably available to you and are themselves considered reasonable.

And that way you can kind of... as long as you can articulate why the action that you did or didn't take at the time was reasonable, then you can still be in line with the contemplated policy that we're considering. So anyway, just wanted to harken back to that helpful suggestion from Brian last week. Over.

PAUL MCGRADY: Thanks, Gabriel. Yes, and we have to be careful that we don't confuse charter question three with charter question number one, right, in terms of the scope of the associated domain names check and the quality of that. And so we should be careful there. It is seven after. We have two other questions we need to get to. We've talked quite a bit about charter question number one already.

And we've got to take all of this and sort of synthesize it into a revised straw man. I see we have Brian, Neha, Marc, Eberhard. And I am going to give everybody fifteen seconds to raise their hand, and then we'll cut the queue off after that. And then we will move on to our next question. So looks like Eberhard's hand went down. Reg went up. Brian, go ahead.

BRIAN CIMBOLIC: Thanks very much, Paul, and really good discussion. I just wanted to introduce another lens to look at the human rights question. A lot of the concern thus far has been taking a look at Article 19 of the Universal Declaration of Human Rights, where we're concerned about free expression, which is obviously very important, and so we need to factor that in.

But I think we also need to factor in the human rights impact of large scale phishing campaigns, where if you look at Article 12 of the Universal Declaration of Human Rights, which protects people against invasions of privacy. And similarly, Article 25, which people have the right for a standard of living and freedom from interference from necessary social services.

And you look at some of the... There was an example that Nominet and the NetBeacon Institute, which is admittedly part of PIR, had something, a campaign that they identified that was targeting UK pensioners, where they had thousands of domains that were registered trying to trick the vulnerable into providing information related to subsidies so they could heat their homes in the winter.

So I do think that while it's obviously important, we have to have a consideration for the human rights of the identified phishers on one side. You also need to balance that against the potential human rights impact of the large scale phishing campaigns for the victims that are divulging personal information, that are finding themselves experiencing interference with social services. So just wanted to introduce that wrinkle into when we look at human rights: it's not just the one aspect as it relates to the underlying registrant, but also the impact of these campaigns.

PAUL MCGRADY: Thanks, Brian. All good stuff. Once we get the... Not that we can't talk about it now, but I think we'll have a dedicated session once we get the straw person stable. And staff will capture all those comments that you've just made, along with some of the others from the NCSG that have been made.

And it sounds to me like that is going to be good stuff for an advisory on how we balance out those things. But we will capture that stuff and include it. Farzi, you are well past your fifteen seconds to raise your hand to end the queue. And so I am going to probably have to hold the

line, but we'll have a chance to talk more about human rights. Neha, Marc, Reg, and then the queue's done for question one.

NEHA NAIR: Thank you, Paul. This is Neha from Radix and also registry side. A lot of what I wanted to say has been covered by Gabriel, so I'll keep it short. But I did want to support the idea of keeping the threshold of one domain, which is well evidenced. Because in reality, the vast majority of abuse reports that come in are single domain reports. There is just no question about that.

Yes, there are times when there are indicators that there might be other domains that could be associated with phishing if it's related to campaign, if the reporter has explicitly mentioned that. But most of the reporters, like ninety-five percent of the reporters, identify one domain and provide evidence of abuse on that domain, and the reports contain no indication whatsoever of whether other domains are registered by the same customer or are engaged in similar activity.

This is not a gap in the reporting. It is simply the nature of how third-party reporters, block lists, or abuse intel feeds operate. So they flag what they observe domain by domain. So I think it is futile to wait for a lot of other reports looking for indicators. That is just going to add delays, and that would give abusers just more time. I wanted to reiterate that. Thank you.

PAUL MCGRADY: Thank you, Neha. All right. We have Marc and then Reg.

MARC TRACHTENBERG: I agree again with Brian's comments, and I won't repeat them. But to Michaela's comments and others, I just can't see how the threshold of one domain name is too low or sensitive. Yes, it's possible that the maliciously registered domain does not have other associated domains, but it is also possible that there are other associated abusive domain names, and this is the entire point of the associated domain check in this PDP.

It is not expected that the associated domain check will find associated abusive domains every time or even maybe most times. But if sometimes that it does, then the benefit of efficiently stopping DNS abuse is accomplished. And I think more importantly, this is actually in the charter of the PDP. So from a procedural perspective, I'm not sure how or why we're discussing this.

The PDP charter says, "This PDP seeks to create an obligation for registrars to investigate other domain names associated with a customer account or registrant where at least one domain name," that's clear, "at least one domain name of that registrant is found to be engaged in DNS abuse as defined in the RAA. To develop a consensus policy that imposes an obligation on ICANN-accredited registrars to proactively investigate associated domain names and/or related orders when a single domain under their management is found to have been registered for malicious purposes." That is clear in the charter. It tells us exactly what we're supposed to do. So procedurally, I don't understand how we're doing something else. That is a different PDP. This PDP says one domain name. That is our trigger.

PAUL MCGRADY: Thanks, Marc. I don't know that we're doing something else. There's lots of ideas. We're starting to repeat those ideas, which is why I'm drawing a line under this particular queue because we've not heard anything new in a while.

And remember, we all made an agreement that we would keep these calls down to ninety minutes once a week instead of four hours a week by not spending too much time repeating ourselves. What we're doing is we're talking it through until we start to repeat, and to see if there's any new idea around which everybody is converging.

If there is not a new idea around which everybody is converging or tweaks around which everybody is converging, then we kind of have our answer. But we do have to talk it through. Otherwise, I understand what you're saying, but if that were the case, then the charter would also not include question number one, right? So it's a little bit circular. They do want us talking about this, and we'll see if we can converge around some new idea or some good tweaks. I think we had some good ideas to kick around. Reg, you are our last contestant on this. Go ahead.

REG LEVY: Thanks. Reg Levy from Tucows. I agree that we have to talk it through. This is what we're here for, this is useful, this is us working. And to that end, the schedule and our ninety-minute sessions should be a guide. If we go faster, if we go slower, that's okay, but the work should be driving us. And simply cutting off conversation when there are still points being

made and still points to be made, I don't think is necessarily conducive to that and to the work.

PAUL MCGRADY: Thanks, Reg. I would agree with that if we were hearing new things. I hadn't heard a new concept in a bit here on the interventions. We've just had people essentially repeating their positions. So if there are new ideas for consideration for question number one or tweaks on how we bridge the gap between the two to three positions that folks have dug in on, I'm happy to hear those.

But absent hearing something new, us spending our time on our calls saying the same things over and over again to each other, that's how we end up with a seven-year PDP. And we've all done those, and they're terrible. So we also have the ability to work in between calls, and we'll encourage folks to do that by taking a look at the straw person language and see if we can make adjustments towards convergence rather than again just putting in the two to three views that folks have dug in on. Michaela, go ahead.

MICHAELA SHAPIRO: Thank you so much, Paul, and I appreciate that. Michaela, for the record, NCSG. I just wonder if having the need to account for the cause and severity of the harm and possibility of associated collateral damage could be integrated into the straw person proposal in some way.

But I also completely recognize, Brian, to your point, that you wouldn't know the full scope of the harm until after the ADC has been done. But I

wonder if, again to my earlier point, if seeing this as a progression, as a kind of proportional view, right? That you do before you do the ADC, "okay, based on what I know now, here's what I can do, and here's the response that is proportional given the information I have right now."

If I see based on that there is enough to do an ADC, and then from that ADC, I find it actually needs to be escalated even more, great, let's do more. That from my view can also get to your point, Brian, about, and completely agree with what others have said, human rights. There's both sides to this. I completely don't want us to be seen as the folks who are also anti-supporting victims of scam abuse. I truly don't want that to be the perception, so I also want that to be clear that I absolutely support that point too. So thank you.

PAUL MCGRADY: All right. Thank you. Let us move on. We're going to take a look at question number two again. So question number two: what criteria should be used to define association between domain names? What elements can be considered to establish such an association? And let me just go through the early input themes that we got.

There seems to be broad agreement from the input groups that you've all heard that there should be a level of flexibility and adaptability to define association since bad actors will change their approaches. Some groups offered concrete examples based upon confidence levels, others non-exhaustive lists, or tiered systems with parts of the tier being contractually required.

The specificity of approaches range from the BC's required criteria to broader flexibility to be determined by the registrars. There seems to be general alignment that association should not be a prescriptive checklist, but some level of exemplary cases and best practices to allow for flexible and adaptable approaches to addressing DNS abuse.

Some themes identified from the meeting and email discussions that seem relevant to question two. For example, some believe the ADC should only be triggered when there are clear indications of associated abuse. We've already talked about this a lot. The counter to the suggestion is that without at least performing some level of baseline analysis, it's unclear how a registrar can reasonably assure that there is zero associated abuse worth investigating.

We think that those are really question three concepts, and so we will get back to that. There is some discussion around the definitions must be flexible since bad actors change their methods. So our definition of "associated" can't be so vague or flexible that it can be gamed or easily circumvented by... it said, "Oh, this is easily gamed by registrars." I don't like that.

Somebody may have implied that, but I think that the registrars on this call are good faith people, not gamers. And/or easily circumvented by bad actors. The circumstantial flexibility is aligned with the notion of requiring reasonable action. And then a suggestion that an advisory can help guide the associated domain name check, which can be updated from time to time.

So again, for purposes of the definition of association, that's what we're talking about here, that the advisory can be updated from time to time. And I'll go back to the gaming thing. I guess I understand why it's in there because not all registrars are on the call, and unfortunately, not all registrars are good actors. But I would just be unhappy if any registrars on this call thought that they were being called gamers because they're not. Okay. So let's open a queue on our definition of associated.

All right, here we go. And it's a fresh queue, so for anybody that thinks they've talked too much, you haven't. It's brand new. Let's go. All right, Reg, go ahead.

REG LEVY: Thanks. Reg Levy from Tucows. So I would like us to focus on account-level relationships because "customer" is too broad for some of us, and "registrant" is too narrow for some of us. So I think reviewing the account is where we should be focused.

PAUL MCGRADY: Thanks, Reg. Volker, Gabriel, Farzi.

GABRIEL ANDREWS: Volker first, right?

PAUL MCGRADY: Yeah.

VOLKER GREIMANN: Yes, thank you. First, before I start commenting on the association, I would like to object against your comment that some registrars are bad or not all registrars are good. I think it is less an issue of them actually being bad actors and more of an issue of them not being educated enough, not being capable enough, not having the necessary information that other registrars have gained over experience.

So I would be hard-pressed to support any statement that basically describes a competitor as a bad actor or as someone who is intentionally supporting illegal use of their services. Even with some of the resellers that we have bad problems with, it is less a problem of willingness and more of a problem of capability.

With regards to the association, I think I agree with Reg, but even the account level might be very difficult to take as the level simply because of the fact that many of us operate in the wholesale space, and what is an account for us may not be an account for our customers. And there is a lot of domains in every single account that have nothing to do with each other other than that they were registered on the same platform. Thank you.

PAUL MCGRADY: Thanks, Volker. So if it's not account, what is it?

VOLKER GREIMANN: Again, multiple things. It could be the same registrant ID, registrant email address, but in some cases, it still may not be. If it is an end

customer platform, then yes, account might be the right one. So there are levels, there are graduations that we have to basically work through. It can be account, but it's not necessarily account. Maybe that helps.

PAUL MCGRADY: Thanks, Volker. And is it a different scheme for direct registrants versus through resellers?

VOLKER GREIMANN: Yes, because obviously we do not have the accounts of the end customers on our platforms.

PAUL MCGRADY: Okay. We need to think about that in terms of registrar business model. I think that's an important distinction, and so we may want to sort of like right from the beginning start to bifurcate that in our heads so that we keep it clear. Because it's two very different ways of doing business for sure. All right, we have Gabriel and Farzi.

GABRIEL ANDREWS: Hi, this is Gabriel Andrews for the record, and I want to actually speak directly to the question you just posed, Paul, that if it is not accounts, what is it? So in the GAC text, we were suggesting that associated domains are those additional abusive domains that are used by the same threat actors and/or used in the same abusive scheme.

And I'm going to paste this into chat here too just to have it easily referred to. But I think this at the high level is very important to call out because you don't want to start thinking about customer accounts or registrants or what have you, because really what you're trying to identify is the same threat actors and the same scheme being employed here.

And that can vary, as we just heard from different folks, depending on the scheme in question. I know some of my colleagues in public safety are already calling out to my attention that very often phishing actors will set up multiple accounts, and this is something that the GAC text also highlighted.

Criminals are smart enough to collaborate. Criminals are also smart enough to set up multiple accounts under their same common control. And so we just want to make sure that any policy we contemplate is flexible enough to accommodate those real-world scenarios. Over.

PAUL MCGRADY: Yeah. Hey, Gabe, before you go, so I guess this is sort of a cart and horse thing again too that I see, because what we're talking about is the definition of associated. And in order to know whether or not a domain name is associated, then under this framework, you would have to know that they're abusive first. How do you know that they're associated enough to go look to see if they're abusive? Do you see what I'm saying? Like, I think this is another one of these things where we tack on a qualitative thing to the end that may not be necessary for them to be associated.

GABRIEL ANDREWS: If I understand your question, Paul, what we're contemplating here is that when you're conducting the associated domain check, that you'd be able to speak in the future to a hypothetical compliance review and be able to defend that the steps that you took were reasonable, right?

And so just as a real-world example, referring to my prior example where you have a BEC phishing actor that has two dozen domains under the same account where they're each representing a different victim, it would be very easy to suggest that it would be reasonable for that registrar to look at that list and say, "Oh, yeah, those are all obviously associated in the same type of scheme if they target different victims."

Conversely, if you had a multiple set of accounts that you're doing your check on and you see that they're all using the same payment data, they're all connecting from the same IP address, and they're registering domains at the same concurrent time period, and even if there are different accounts, that they're all following that same pattern, that would be another way of identifying that that is the same abusive scheme.

It's a different set of facts and circumstances. We want to ensure that we're not being too prescriptive about what those facts and circumstances are, but rather have a common understanding that the registrar will always make use of the information available to them without necessarily being compelled to list out what that information is.

The facts and circumstances will change. What has to happen is that the registrar makes use of the reasonably available information and that

they can defend the actions and the choices they make in the future. Over.

PAUL MCGRADY: Thanks, Gabriel. So I guess this is the problem of being married to a rhetorician. Do we need the adjective "abusive" before domains? Are those additional domains used by the same threat actor? Because if we say they're the additional abusive domain names, then you've got to determine that they're abusive before you can have an obligation to consider them associated, right? That to me seems like you're in your own way there. But if you want to keep it, that's fine. But it seems like an adjective that creates a problem for you.

GABRIEL ANDREWS: I'm not sure that it does. We can contemplate that more on our end; I'll take that back. But I think that my initial reaction, Paul, is that as you're doing this associated domain check, I mean, that is the crux of what you're checking for, is to see if these domains are used in the same abusive scheme or not.

It is theoretically possible, to Farzaneh's point, that your malicious phisher might set up ninety-nine domains that are used in phishing and one for a home blog, and I don't necessarily care about whether or not that home blog is taken down or not. I do care that you're minimizing victim harm with all the other potential victims that are being targeted. And that's... I guess I'll pause there because I want to go back and reflect on that question. But there's no initial adversity to that from my end, speaking at the personal level. Over.

PAUL MCGRADY: All right. Thanks, Gabriel. Yeah, I think it's important to remember what we're doing is we're essentially defining what "associated" means. And we've talked about all kinds of sort of objective things that you don't need to really know what's going on with the domain name to know whether or not they're associated before you can look at them, right?

Those are things like shared payment, shared IP, same registration date, registrant in the same account. Those are all good stuff that I think would populate an advisory. But if you have to know that they're abusive before you can know that they're associated, then I don't know how that works. So anyway, thanks for taking it back. Farzi and then Anil.

FARZANEH BADII: So I am very interested to understand when we talk about accounts, what we are talking about. Because, and the registrars can tell us better, but as Volker puts it here, when we say account, like Wix is an account holder and they have so many domains there.

So I just want to have a better understanding of how we can define this within the registrar's different business models. And also like Bruna said, what Gabriel is saying is a little bit concerning for us. Yes, we also care about the victims.

I don't understand why there is this impression that we are cherry-picking on rights. Obviously, we are saying that we need to look at the severity of the harm so that we don't redirect our resources to some

kind of abusive domain while we are leaving the victims that are being impacted behind.

So I am going to write an email to the mailing list about how we address these issues and how we address human rights, and we actually care about victims as well. But one thing that I would like to understand is how a registrar's business model can have an impact on what level of associated domain we are talking about.

PAUL MCGRADY: Yeah. Thanks, Farzi. I would too. You know, I think if we can get a volunteer from the registrars to do... I'd love to see a little chart put out on the mailing list about what different kinds of registrar business models provide what visibility into who the registrants are.

Because I think that's going to be really, really important here because if we have two distinct business models where one is direct and one is through resellers, we don't want to define "associated" in a way that doesn't work for both business models. I think that that is important. So, Anil, go ahead.

ANIL JAIN: Thank you, Paul. Anil for the records. We are talking about the definition of associated domain. So one thing I agree with all the previous speakers that the "same account" means that whatever we have written in the WHOIS form, if the things should be matching, then that can be taken as a same account.

The second thing which I am now talking about is maybe different altogether. Number two is that even if a domain is purchased by the same registrant, maybe with the same name or email or address or something, but we have not got any information about whether that domain is abusive or it is likely to be abusive, can we take that as associated? This is one question which I have.

And second is that suppose the registrant has not the same... is not having the same account, but there is a similar pattern of abuse which we have observed in the past where the registrant is directly or indirectly involved in the process. So can we also take those domains which a registrant is holding today as associated? So this is slightly extending the definition of an associate. Thank you.

PAUL MCGRADY: Thank you, Anil. Staff, if you can do me a solid and go back to slide fourteen so that we... I think it will just be easier to hold in our heads that what we're talking about is we're defining the word "association," right?

And this is the opposite, I think, in some respects of question number one, because I see zero possibility of a happy future that does not consist of answering this in a way that can be quickly updated and changed by advisories rather than trying to bake this thing in hardcore, right?

And so the advisory, I think, has to be structured along practical lines based upon registrar business models or else it is not going to... that's not going to work either. This seems simple. Like, "hey, what are

associated domain names?" It turns out it's not super simple. And so let's... I think having the question up is helpful. All right, we have Volker, Marc, and then Reg.

VOLKER GREIMANN: Yes. Thank you, Paul, and you're absolutely right in what you just said. We need to have the association part be very flexible and pliable to make sure that it can stand the test of time. Because if we limit ourselves to account or registrant, that only introduces different kinds of abuse that we're already seeing.

To just give a couple of examples, a lot of abusive patterns that we see have no similarities in the registration data, no similarities in the email addresses. They're all taken from phone books. The registrant data is taken from phone books and then applied to one single domain name, and checking the registrant or the email address will gain you nothing.

There are other association pointers that we are using to identify those domain names and that help us... that are absolutely belonging to the same campaign, but we wouldn't be able to associate them through the registrant.

There is one large darknet website that we're chasing at the moment that goes through different resellers, different registrars of ours even, through various intake sources that we can recognize by various patterns that we wouldn't be able to do on the registrant or account level association checks.

Therefore, having an association terminology that allows or requires even checks that go beyond these two criteria is essential for us, because that only... only that allows us to dig deeper and make sure that the policy we're developing as a group is fit for purpose and future-proof.

Because if we're saying registrant must be the same, then there will be just more identity theft and a lot of people complaining to us that people are registering domain names in names of people that have nothing to do with those. And that is already occurring. Thank you.

PAUL MCGRADY: Thanks, Volker. All right, Marc?

MARC TRACHTENBERG: I agree with Volker's comments and, you know, I think that there's various tactical and other reasons why we have to get the association right and kind of have maybe minimum standards where there is some discretion for the registrars to also decide what might be reasonable in a particular case.

We don't want to have it be too narrow or too broad, and we want to leave flexibility for people to be able to conduct their investigations to adapt to how the bad actors are engaging in DNS abuse.

But the one aspect that I still really just don't get is I keep hearing about the comments made about surveillance and proportionality and why this is taking into account the potential harm of the account owner or the registrant, and I'm just struggling to see what that harm is.

I mean, keep in mind here again, we have a domain that is intentionally used for DNS abuse. We're not talking about exposing any customer data or any other data or domain data to any government or police or any sort of authority or any external party whatsoever.

The only party that is seeing or doing this check is the registrar, and the registrar already has access to all of this data. So they can already run the ADC if they want to voluntarily for any purpose whatsoever and do whatever they want with this data.

So this is where I just don't see... even if the association definition were to be broader than some would like, I don't see how that negatively impacts any registrant since, again, it's only the registrar doing this check, and the registrar already has access to this information.

PAUL MCGRADY: All right. Thanks, Marc. Reg and then Tomas.

REG LEVY: Thanks. Reg Levy, Tucows. The presumption that we have access to information or that we can search using that information is where I'm having a concern. So if there are four registrars under my purview, and in some of them, I can easily search by email—email, not address. In none of them can I easily search by name.

So when somebody comes to us and says, "We want you to delete all data that we have," I can't just do a search for John Smith and then delete all that information. I have to have the email address that is associated. So, and even then, it is very difficult and not something that

my team can just do every time there's a DNS abuse report that comes in.

Going toward Brian's example about how there is, like, IRS, but it uses the Turkish I, so there's no little dot above it, and that this is how that particular campaign was being conducted. We can look at the account, we can look at the account that the domain that was reported was in, and we can see if there are similar domains that we think might be similarly related or similarly abusive or even not similarly abusive; right? One's IRS and one's a fuel issue for Ireland.

But what we cannot do is just say, "I wonder if John Smith registered other domains at other resellers, at other even registrars that are under our purview." So I want to make sure that we aren't hung up on defining even the association. It should be reasonable for each registrar, reasonable for each of us that the association exists and that we can search for it.

So from my standpoint, if we're going to go down any road, we should be going down the account road and not even talking about or looking at registrant. But there are some registrars that could even use the IP address, and that that would be even more granular. And that is reasonable for them in a manner that it is not at all reasonable for me.

And someone in the chat said, "Well, we need to have more information about business models." And yes, I'm happy to help provide that, but we also... all four of my registrars have the same business model, and we have a similar business model to Teo and Volker, and yet our databases are structured very differently.

So it's a matter of the database structure, it's a matter of the business model, it's a matter of how the system actually works. And just saying, "Oh, just search for the registrar," is not necessarily something that we can do. So account if we're going to do anything, but in all cases, reasonable for the registrar in question.

PAUL MCGRADY: Thanks, Reg. Tomas, go ahead.

THOMAS RICKERT: Thanks so much, Paul. I hope that my audio is going to be all right since I'm outside. Some of what I was about to say has been covered by Reg. I mean, what I find difficult with this discussion is that we're trying to do a human rights impact assessment on the fly without knowing what the concept even is.

And I think that we should discuss what we think is the right approach and then have a small team conduct a data protection impact assessment as well as a human rights impact assessment, because there are many more factors that need to go into such assessment, you know? So I think maybe we can step back, try not to do everything at the time and in real life mode, but discuss first what we think is most useful and feasible, and then look at the legal aspects of it.

PAUL MCGRADY: I completely agree. We need stable language. I mean, we can certainly discuss it, you know, in a lightweight way as we go. But without stable language, I don't know how you can do a human rights assessment on

language that everybody's not agreed on yet. Not a fulsome one anyway. We can certainly spot the red flags as we're discussing it. Ching.

CHING CHIAO: Thank you, Paul. This is Ching. Sorry, my voice is a little bit off, but hope you are hearing me okay. I would like to echo what Reg and Volker pointed out, that the registrar should definitely have a reasonable way to determine the ADC, their methods.

And I'll also like to emphasize, because this particular question number two about the association is for one single registrar. But obviously the question is a broad question about the... I mean, so I would just like to simply remind members here that we're talking about finding out associated domain within one single registrar.

My last point here is that, just to share one example about finding out, I mean, one recent case I personally deal with, finding out ADC domains definitely need to allow, once again, registrar to have reasonable methods to determine.

One recent case that I worked on is that multiple registrants, multiple accounts, nothing similar. And then the pattern that we found is that a Bitcoin address, multiple Bitcoin addresses were used in the subdomain stream.

And some of the researchers of ours and our colleagues were able to find the patterns simply like reading the subdomain. So nothing on the email address, IPs. It's just, you know, sometimes it is based on the experience or sometimes based on hunch that, you know, when

registrars are doing the investigation, they are able to pull some of the resources or some other stuff, they are able to do it. But so I'd just like to put that example out for your reference. Thank you.

PAUL MCGRADY: Thank you, Ching. All right. We have Rod. Go ahead.

ROD RASMUSSEN: Yeah, thanks. So I think this discussion and especially what's been going on on the chat have been helpful here in kind of identifying that there are a myriad of ways that things can be associated, and there are a myriad of ways in which different registrars may have access to different kinds of data.

I think what would be good for framing this are instances and trying to determine what is reasonable for a registrar to have taken action in an ADC type scenario with looking at what they associated with that initial domain, if it's been triggered.

So what is, you know, at the end of the day, have you taken the information you have along with information that is known in general as to how things get associated and done a reasonable job of looking at that? And not... I think part of what we get wrapped around the axle about is what must be done.

And that's... I don't think there... we will end up with "every registrar must do this action" based on a trigger. It would be very hard to coalesce there. But if we can come to a situation where we can

determine what are reasonable associations to have looked at and being able to do that, that would be helpful.

One thing I would suggest we take under consideration that hasn't been mentioned on the call yet, that I don't believe, is that sometimes you will get a report in of an abusive registration along with, "Hey, this is associated with this campaign, and this is what the thing is to look for. This is what the association is."

I would argue that under that circumstance, it would be pretty hard to argue that you were not doing a reasonable check if you determined, yes, that was abusive, and you didn't then take a look at the provided evidence for associated domains where you were actually given what those associations were. And I'd like to use that as a conversation stimulus. Thanks.

PAUL MCGRADY: Thanks, Rod. All right. I don't see any other hands. Going once, going twice. All right. Lots to think about here. It seems to me that the primary thing for leadership and staff to do with this is to gather up the various elements, right, that were kicked around as things that could be considered to establish association.

It sounds like I didn't hear anybody arguing for a hard and fast unmovable definition of, or rather criteria of, "associated," based not only upon different registrar business models, but also based upon trying to find a better word than bad guy. Threat actors or threat based upon how quickly unsavory types move.

And so we'll do some thinking about that and put together a draft list. In the meantime, if I can, on this particular item, do request a registrar to put out something on the list that sort of clearly delineates the business model.

I see two: direct to registrant, and I see through reseller. There may be something else out there. So if there is, if we can capture all those, I think that would be helpful. We have nine minutes left. I don't think it will be valuable to spend six minutes trying to jump into question number three.

All it's going to do is we'll have one or two speakers, and we really won't have a conversation. So we are going to stop here unless anybody else has any more comments on question number two. I've not seen a hand in a while, so last chance there. Okay. Let's go on then to... Oh, Anil, go ahead.

ANIL JAIN: Thank you, Paul. My suggestion is that we had a big discussion on charter question number one and charter question number two, and we are able to gather a lot of observations from members in this chat.

Is it possible to consolidate for both charter question number one and charter question number two and share with all of us? And in case we can have comments before the next call, that will be quite useful. Thank you.

PAUL MCGRADY: Thanks, Anil. Yeah, we will certainly be taking a look at the current straw person. Let's go on, folks, to next steps. Staff, we can go to next steps slide. We will be... staff and leadership will be updating the straw person for question number one with the learnings from today's call, and then we'll send it out.

And we'll be encouraging people to take a look at it to figure out how we smooth out the issues that were raised there. Tomas, I saw you actively attempting to do that in the chat. I wish I could listen and also do chat the way some people can. I'm terrible at that. I will read through the chat, of course.

But Tomas, maybe you can weigh in on some of the things that you were typing in there. I thought they looked great, and certainly will help us further refine that straw person for question one. Staff will populate the collaboration document with all the various comments made.

I also think it would be helpful if leadership and staff put together at least an initial draft of the various elements that could be considered when looking at whether or not domain names are associated with each other. There are a lot of good ideas that were thrown out rapid fire, a lot by Volker. Thank you.

And if we can have the business models, if somebody could take a look at that and throw that out just by way of... as a piece of information for those of us that are not registrars, super helpful.

So once we get those things out to you, if the working group can look at the collaboration tool and provide the feedback on that for question number two. We didn't get to question number three. The good news

about question number three is we've actually secretly talked about it because we kept wanting to jump from question number one to question number three.

So when we get there, you'll see that the discussion there is already quite advanced. But take a look at question number two in the collaboration tool. And if you have things to add to question number three, that's fine too.

And we will get ready to talk again next week. I think we're back on track for Monday next week. I have five minutes. Staff, do you have anything to add? Or Nick? Or Jen? Okay, everybody gets five minutes. This is great. Thank you all. This was a robust conversation. We are making progress. I promise. All right. Thank you. Bye-bye.

[END OF TRANSCRIPTION]