ICANN85 Mumbai | CF – GNSO: DNS Abuse Mitigation PDP1 Working Group Session (4 of 4)
Monday, March 9, 2026 – 15:00 to 16:00 IST

ANDREW CHEN

Hello and welcome to the DNS Abuse Mitigation PDP-1 Working Session 4 of 4. Please note that this session is being recorded and governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning statements of interest.

Please observe the following guidelines to participate in this session. I will post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during this session, as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand the floor over to Paul McGrady.

PAUL MCGRADY

Thank you. Good morning, good afternoon, good evening, wherever you happen to be in the world. I am Paul McGrady, and I am nearly chair of this PDP. Our temporal anomaly is hopefully coming to an end here in a couple of days, but in the meantime, we're just forging ahead.

So, this is session number four, and we are going to get to work. So, this is the part where I say, if you went off the jumbo jet, now's your

chance because it's about to take off. So, we're going to talk a bit about the scope methodology and then we are going to go ahead and start answering charter question number one.

So, in terms of scope, we've talked about that in our very first session. The scope is the Charter. It is the nature of our universe. We will not be expanding outside of the universe.

Volker has already come up with a good idea about how to capture our good ideas, which are not contained in our universe. And so, we should be thinking about those along the way as ideas come to us that we think councils should feed back into their DNS abuse small team, which could then result in a QPDP, a quick PDP or whatever this is.

Then we should be gathering those and we're going to talk a little bit more about that in the near future about how to capture those ideas without expanding the scope of our work and without slowing us down.

In terms of methodology, I'm going to throw out something that I think should be our lightweight methodology and I'll take a short cue on that and then we'll get on with Charter question number one. So here is my proposed lightweight methodology, which is we answer the question and from the answers of that question, then we have staff in between the meeting where you answer it in the next meeting, put together a draft recommendation for us all to consider. And then we consider that recommendation.

We then do a lightweight iterative impacts review, taking a very high-level look at human rights issues about bouncing into other ICANN policy. And there was one other impact, which I can never remember. I apologize. But we kind of do that on an iterative basis, rolling so that we're not surprised at the end and so that we also don't say, we don't create an opportunity for us all to re-litigate everything at the end, because we didn't look at this at the time we were doing it.

And then we declare something 95% static, we draw a line under it, and then we know we've answered question number one, and we have a workable recommendation for question number one, and so on and so on, right?

And there will be overlap as we -- we'll go back and forth between answering the next question and looking at the recommendations from the last question, the draft recommendations so there'll be some back and forth. It won't be all in a straight line. It's going to be two steps forward or one step back as we go.

So, I'm thinking that that is a good way to do this and we'll give us some certainty that once we get to the end of answering the questions, we will be 95% done with the work. And then we can go back and do, you know, more heavy duty looking at the impacts and those kinds of things just before we put together our initial report. So, I have two people in the queue so far, but jump in. Feodora, please go ahead.

FEODORA HAMZA

Thank you, Paul. This is Feodora from ICANN org. I just wanted to add a few more details on how we're going to capture working group input and discussion.

So, there will be a Google Drive where all the work, the draft documents will be saved and the working group will have access to them. Furthermore, there will be a working document. After each session, we would ideally have some key takeaways, and based on those key takeaways, we would then propose or have the group react to some draft language that they all can review after each session and provide comments and react to each other so there is enough room to operate and collaborate outside the meeting.

And as Paul said, there will be then also a section later on where we would compare against the impact assessment, but just for more detail on this.

PAUL MCGRADY

Thank you. Yeah, there will be at the end a more heavyweight look at the impact assessments, but I do think we should look at them iteratively as we roll. Before we get a draft recommendation back out to the team, I will have looked at it with staff and your vice chair, whoever that turns out to be, will have looked at it with staff. And it doesn't preclude anybody from rejecting it entirely or evolving it or whatever we need to do, but that's sort of the thing.

Our work in between will consist largely of looking at those written documents and smithing as we go and that's that, when we talk about the homework, that's what we mean. primarily. All right, we've got Anil. Go ahead, Anil.

ANIL KUMAR JAIN

Thank you, Paul. Anil, for the record. Regarding the scope and methodology, I'm just taking a step before you deal upon the methodology and scope. See, you have done a wonderful job in asking the SOs and ACs and you have given five questions to them to answer those five questions and I think that is a very important step which this PDP has taken through you.

So, we must take inputs from all these SOs, ACs because the last date we have given is 20th of March and we should take this as the feedback from the ICANN community through us, through this PDP, to make the base of it.

The second suggestion which I want to include in front of all the community here is that we are focusing on registrar and DNS abuse related to the operation of the registrar.

I personally feel that yes, we have a representation from the registrar strategy group, but at the same time, in case we can invite a few other registrars who have got impacted because of DNS abuse in the last three, four years, that we should hear from them that how they got impacted and what mitigation measures they have taken to reduce these kind of abuse in future.

The third thing I just want to remind that ICANN had issued recently some guidelines about the functioning of PDP. Those aspects we should also consider and we have a charter which is already defined.

So, these four legs of the base which is available with us, once we are through with this, we should draw the boundary lines under which we have to operate. And I fully agree with you, Paul, and your approach that whatever discussion we do in the PDP, it should be focused, it should be pointed, and it should be time-oriented.

And finally, once we draw those lines, I think we should also draw the targeted timelines by which -- although the timelines we discussed in the first session itself are there, but we should further divide those timelines and we should try to restrict ourselves in those timelines. These are a few suggestions which I just wanted to place in front of all of you. Thank you.

PAUL MCGRADY Thank you, Anil. All right. Let us then jump in to Charter question number one. Okay. So, Charter question number one is, what triggers the requirements to investigate associated domain names? All right, let's do a queue. Brian.

BRIAN CIMBOLIC Thanks, Paul. Hi, everyone. Brian Cimbolic, PIR. I just wanted to note for context, and I'll put it into chat, the sort of status quo of -- and I realize I'm not a registrar, so I want to give Volker a chance to,

but what triggers an obligation for registrars to mitigate DNS abuse right now, that's set forth in the contract, the RAA section 13, I'm sorry, 3.18.2.

And so, I think that in these discussions, that's probably a good place to start because an associated domain check has to be conducted on a domain that the registrar has already been identified as engaging in DNS abuse. So, at least contractually, we're not starting from scratch. There's a place to start in the contracts.

PAUL MCGRADY: Thanks, Brian. Maybe we can put that -- I think someone's already beat it to me. Yeah, Brian, there you go. It's in the chat, 3.18.2. I know each of us reads that at night before we go to bed so let's start to memorize that. All right. Volker.

VOLKER GREIMANN: Yeah, tying into that because that's basically already covered by this, let's start with the lowest hanging fruit here. Any evidence or other indications that there may be such other associated domain names?

So that may be experience that we have with previous registrations, multiple tickets for abuse that indicate that there's a nest or a grouping of domain names. Anything that indicates to us or provides evidence that there are such domain names would trigger such an investigation requirement.

PAUL MCGRADY Thank you, Volker. Other hands, other comments? Ching?

CHING CHIAO Thank you, Paul. So, I guess as of now, we're kind of, as you just pointed out, we're in this working mode of trying to respond to this answer, which I believe that it's naturally to start with the RAA.

But also on the other hand is that in the real world, you know, businesses, I mean the real-world evidence that we're seeing right now is a lot of like what we call a slow burn which means that the ADC is found, but it's nothing maybe a seed domain or root domain is found with phishing evidence. But a chain of other names and cluster of other names maybe fall also potentially in that, you know, potential category.

So, what I've heard, it kind of makes me want to jump right in into that. Actually, on one hand, is that I fully agree with Volker, is that we should start with dealing with the low-hanging fruit. That's for sure. Fully support on that. But I also don't wish to exclude the opportunity of, you know, eyeing on other possibilities of if we can do better this time.

PAUL MCGRADY Thank you, Ching. Anil, and then Jothan.

ANIL KUMAR JAIN

Thank you, Paul. Very interesting part. One, of course, is the associate domain name is being investigated by a large number of registrars and registry themselves. So I think first is whatever information comes from a regular complaint or observation that a particular domain is being used or potential to be used for DNS abuse, that gives a trigger to investigate other domains associated with that particular domain. I think this is first.

And second, in case we find that registrar who is holding a domain, some unusual activities have started from his account or her account. For example, booking large number of domains or booking domains which are of special character.

For example, somebody using 123, 123, 124, 125, and they register 500,000 of domains together, that gives a suspicion that these domains are probably expected to be used for not normal activities. So that gives say a trigger that a registrar should enter into the investigation of all associated domain names of that particular registrant. So, these are my initial comments. Thank you.

PAUL MCGRADY

Thank you, Anil. We have Jothan.

JOTHAN FRAKES

Yeah, hi. I'm Jothan Frakes. So, I am a registrar, but I'm participating in this group as a member of the SSAC. What I'll say is, you know, we had some good, I think, starting point from Brian

related to 3.18 and what that looks like. So that's the trigger in the context of our policy.

But the question was, you know, what triggers the requirement, this is not necessarily a requirement, this is what would trigger an investigation, might be a notice from a credit card processor for the registrar that a stolen card or a fraudulent card was used, then we may start to investigate other things.

So, there are other things, but those are going to vary by registrar and they're going to vary in other ways. So, there are triggers beyond just that report. We're starting with the focus of evidenced report where we've taken mitigation steps and looking beyond that, but there can be other signals. Thank you.

PAUL MCGRADY Thanks Jothan. Reg.

REG LEVY Sorry, I forgot that I raised my hand. This is Reg Levy from Tucows. I think that whether or not a domain was registered at the same time as another domain is not something that is readily available at the time that the determination that one of the domains is malicious is made. So that may not be the best indicator in that regard. And it seemed like Anil was pointing toward bulk registrations themselves as being malicious, but I think that's a different PDP.

PAUL MCGRADY Thanks. Yes, there is PDP2 coming down the line, I think, that's looking at, I'm afraid to use the word bulk because I know bulk is like a lightning rod word. I don't know why it is, but I don't want to use it, so I won't, but whatever that is, yeah, it's going to get looked at, right? Somebody is IGF Secretariat. I don't know who that is, but if you could identify yourself, that'd be great. IGF Secretariat, are you there? All right, we're going to go on to Vivek. Go ahead.

VIVEK GOYAL Hi, Vivek Goyal from the BC. The way I see it is there can be two triggers. One is an external trigger and an internal trigger. The external trigger is what was mentioned. It's written in the RAA as 3.18.12, where the registrar receives a complaint.

Now, they have an obligation to review that complaint, and that might start an associate domain check, but can we discuss if there is an -- and I don't know the answer, I'm looking at my colleagues at CPH to see, is there an internal trigger which can also start an associate domain check? And if maybe they can elaborate whether they have such internal triggers to start a domain check, and that would then internally start an associate domain check. Thank you.

PAUL MCGRADY Thanks, Vivek. We have Michaela.

MICHAELA SHAPIRO

Thanks. I can't answer Vivek's questions per se, but I just wanted to come in on a couple of small things just to say, reiterating where Brian started just having making sure that we are looking at the contracts.

Already as a starting point, just wanted to remind folks that we also do have a clear definition of DNS abuse, obviously, that we can also discuss further if needed to clarify for specifically the purposes of the associated domain check. But also, just putting it out there that that should also be a starting point is looking at the definition as defined by ICANN of what is DNS abuse to help us stay on track.

And similarly, to just back up Reg's point as well related to the question of bulk registration, just that that is a separate topic. So, I just wanted to make sure that we stick to the scope of the charter here on that topic as well and that that's a lovely topic to be handled later on. Thank you.

PAUL MCGRADY

Thank you, Michaela. All right. We are going to go back and ask the IGF Secretariat if they're there. Anybody identifying as the IGF Secretariat, this is your last call. I'm going to start ignoring you soon. All right. Moving on to Martina.

MARTINA BARBERO

Thank you very much, Paul. And apologies, I'm trying to make sure that you hear me well. Thank you very much for this discussion. I think we heard already very interesting thoughts. I have to

acknowledge that within the GAC we are still discussing our initial input to the early question. So, what I wanted to share are a few reflections that we've exchanged in the DNS abuse small group.

And I think as an internal trigger, it was acknowledged by GAC members that the RAA, so the recent contract amendments, in fact, are a good starting point. So, whenever there's actionable evidence, as referred in the chat, that could be one of the possible triggers. And we're also discussing still at the brainstorming phase what could be other triggers in case of suspicious behavior or other suspicions that something is going on. So that will come later, but just to acknowledge that for the moment, this is the state of our reflections. Thank you.

PAUL MCGRADY Thank you, Martina. Brian, back to you.

BRIAN CIMBOLIC Thanks, Paul. Brian Cimbolic for the registries. I think it's important to remember the distinction between cases and referrals and actually confirmed instances of DNS abuse.

We get false positives. I can't speak for registrars, but I know that they do often receive false positives. Registries, we certainly receive false positives. So, I think it's important to then think about then, okay, you get external reports and registries and registrars, Vivek, are required to have web forms or emails to receive external complaints.

So, let's take a fact pattern where a registrar receives a complaint, sees that there are 30 domains listed there, but none of them are actionable, none of them are under their policy it would be kind of absurd to then require that they look for further false positives.

As opposed to they get an actionable evidenced case of DNS abuse, a clear phishing domain. And under the RAA currently, they would absolutely be required to mitigate that domain. They would client hold, they would delete, whatever they would do to mitigate that domain, that is when the obligation should likely kick in. It's associated with existing DNS abuse, not claims of or reports of DNS abuse, but confirmed DNS abuse under 3.18.2.

PAUL MCGRADY Thanks, Brian. Anil, go ahead.

ANIL KUMAR JAIN Thank you, Paul. Just commenting to the comments of Vivek Goyal, yes, I agree with him that there are two triggers. One is internal and one is external. I think we have got a lot of inputs about the external trigger, but there are internal triggers also, Vivek.

Like in the morning, we discussed from the PIR that they have tools to investigate a domain whether that is involved in DNS abuse. We have another tool which is called DAR, which is internal to ICANN and which is used in RIRs. And there are other abuse reporting tools

which are being used by various registries and register for internal use.

And whenever such thing happens, then we have to follow the process of talking to the registrar, talking to registrant, and then intimating them with the confirmed evidence that this is there, and then we can take further action of mitigating them or removing that from the root. Thank you.

PAUL MCGRADY Thank you, Anil. We have Lawrence.

LAWRENCE OLAWALE-ROBERTS Thank you. My name is Lawrence from the BC, a member of the PDP, sorry, participant to the PDP. In a number of cases, in a lot of cases where DNS abuse is established, I believe there is a handshake with a hosting provider. I mean, the domain has to be hosted somewhere. And to a large extent, there is a lot of activity that goes on the hosting side that can be an indicator that someone is using that server or something to spam.

I don't know how the handshake is with the registrars, but I believe that that could be an indication that there is some activity going on that needs to be investigated. Possibly we can have some clarity if this is a real-life scenario that works out.

PAUL MCGRADY Thank you, Lawrence. All right, Vivek.

VIVEK GOYAL

Vivek Goyal for the BC. I'm going to share this situation and I can get some feedback from colleagues at CPH. Generally, what we have seen is criminals register multiple domains and activate one of them. By the time you realize that it is phishing and report, they have already accumulated enough wealth of it and turn it down and then after some time, they activate another one.

So, imagine a scenario where they've registered 50 domains and we report one to you, by the time it reaches you, right, it's already down. So that means you have no obligation to check the other domains. But if you did check the other domains, you might find that most of them are activated and are doing phishing. So how do we resolve this?

And I truly understand, you cannot look at all the domains for every complaint you get, but this is a real-life scenario which we have seen happen, right? So how do we resolve this and make ADC part of this so they can handle this situation? Thanks.

PAUL MCGRADY

Thanks. That's an interesting question. I'm looking forward to hearing the answer. Volker and then Martina.

VOLKER GREIMANN

Yes, I think that's an interesting question, but it probably goes a little bit too much in the weeds and we should probably focus on that later, but there are ways to make us look at those by providing

better evidence. So when we see a domain that has been deactivated, then the evidence package that is provided to us with a complaint is the deciding factor of whether we take action. So, there are ways, but let's delve into the details of that at a later stage when we come to the points and suggestions that we will end up on.

For us as contracted parties, one trigger that's maybe not a requirement, but also a trigger for investigations that we do is business reality. Looking at abuse complaints takes time, costs money. Therefore, we want to reduce the number of abuse complaints that we receive. The best way to reduce the number of abuse complaints we receive is to reduce the number of abuse domain names on our platform.

Therefore, it is in our own very special interest to make sure that when we find a domain where there is likelihood of further domain names being registered for the same purpose, to take care of those domain names in the same action that we take care of the one that we have just received a report for. Meaning that we will not receive reports for the maybe dozen, twenty hundreds of other domains that they may have been registered.

So, we have established internal processes for domain names that either are covered under the RIA or violate our terms of service, that we have regular checks for certain patterns that we've established, be it fake shops, be it darknet marketplaces that we do not allow,

be it phishing domain names when they have certain patterns that we recognize and that we have seen before.

We might even have weekly run-throughs of certain reseller accounts to make sure that there's no new registrations of the same pattern in our own special business interests. Not because we have an obligation to do so, but because we feel it's A, the right thing, and B, it saves us a lot of time and money to do that.

PAUL MCGRADY: Thank you, Volker. So, we'll capture the question of is being used versus was being used, right? So, Brian, I'm going to put you on the spot after we hear from Martina on that question, because that would be an evolution of what's in the RAA. So, I think there's a thing there. Martina.

MARTINA BARBERO: Yes, thank you very much, Paul. And indeed, we wanted to, as a GAC, try to understand a bit more this point of to what extent is this useful to look at other domains to investigate the report of abuse on one individual domain. So we have heard from Theo earlier today, and that was very helpful that, you know, in the case of people of campaigns, you can see that there are many similar domains that are registered with a similar string for the same purpose.

So maybe you receive as a registrar a report for one of those domains, but let's assume that there is no fake web shop yet on the

page. So, you don't know further why this domain would be used, but then all the other domains are already showing very nice pictures from the payment fees of the UK government or other similar phishing campaigns.

So, you would look at the other domains and see, oh, indeed, you know, this domain would be used for abuse. Would that be useful as an evidence? We're just trying to educate ourselves on this matter at this point.

PAUL MCGRADY: Thanks, Martina. And so, we've heard from Martina and Anil both, and theirs is might be used for DNS abuse, right? So, we have is being used, was being used, and might be used. Brian, I'm only going to put you on the spot for was being used.

BRIAN CIMBOLIC: Sure.

PAUL MCGRADY: But if you want to address the other one, too, that'd be great to do. Sorry to do this to you, bud, but you're the one that put the agreement portion in the chat.

BRIAN CIMBOLIC: No problem. Happy to take it. So, Brian Cimbolic with the registries. Let's, again, kind of ground things back to the status quo. The current status of the registrar accreditation agreement,

as also the registry agreement, the standard is actionable evidence that the domain is engaged in DNS abuse. And we do this for a number of reasons.

One of which is that upstream, downstream, I'm not sure which way up the stream, if the site is no longer resolving content, then the harm may have been mitigated by the hosting provider, or the bad guy may have taken the stuff offline.

So, there's not really, at least I'm not the most technical guy, I would admit, there's not really a good way to differentiate that. And so, when the registrar or the registry looks at a referral and there's no longer content resolving, we can't say that there's actionable evidence that the domain is engaged in DNS abuse.

And so, I do think that that's a pretty fundamental change. And I think that to take action on a domain because it might engage in DNS abuse, I think that's pretty dangerous territory that you really need to be pretty sure because when you take action via the DNS, there are all sorts of consequences. The mail stops working, at least if you apply server hold, client hold, the domain and all the associated uses for it go away. So, you have to be very careful.

It's not to say I'm very much in favor of mitigating DNS abuse, but I think that we were pretty deliberate about the standard in the agreement, and the standard is actionable evidence of DNS abuse.

That also makes it easier to scale. Registrars get tons and tons of abuse complaints. And so, if the burden shifts from concrete

evidence that this domain is engaged in abuse to much squishier, harder to justify, this domain could be used in DNS abuse, I think that it becomes really hard to actually continuously apply that in a way that is, I just don't see how it would operationalize.

PAUL MCGRADY

So, let's set aside might be for a while and talk about was for a little bit more, because is I get right, you can go and you can see what's happening and oh, yeah, that's bad. But what happens if somebody like Vivek says, reports it?

By the time the report gets to you, it's no longer resolving, but they put together a decent evidence package and it looks like some bad stuff was going on. What do you do with that one? Do you just say, eh, it's not in the contract, or is there a next step? So, Reg, you're going to take this one? All right.

REG LEVY

Yeah, so it may depend by registrar, but if it turns out that it's something that we would suspend anyway, we would suspend it, and then we would have taken action, and then that would prompt the review. So it's from my standpoint, what we're discussing here is when there's an action taken that we've determined a domain is bad, then we go look. So, if we look at the evidence package and we're like, well, we can't tell, we move on with our lives.

But if we look at it, and even though it's been mitigated already, we're like, yeah, this is bad, and we're going to terminate it already, then we will take that action and then that would be a trigger.

PAUL MCGRADY Thanks, Reg.

REG LEVY Reg Levy, Tucows.

PAUL MCGRADY Sorry. All right, Ching, back to you.

CHING CHIAO Thank you, Paul. Also going back to my points on the slow burn and your point on the might be, the part is that in the real-world cases so far, for example, a lot of cybersecurity company that some of us work with is that slow burn means that, for example, a cluster of names, let's say 100 names, maybe one got found, right?

And then a lot of what we call the NRD, the Newly Registered Domains, the NRDs, will simply get blocked by the cybersecurity companies simply because of the age of the domain. So that probably will be done by the cybersecurity company level, their solutions to their customers, so on and so forth.

So, some of the names registered by the bad faith actor, let's say that 100 name, they may not be able to, or they may not activate,

for example, 50 of them. They will just keep wait and see, you know, trial and error if the first 50 got shot and then they will activate another 10 or 20 just to see how things work.

So those trial and error, what we call the burn, I mean, the slow burn kind of period. So, the question actually throws back to us here is that whether we should take action earlier or should we just keep waiting to collect evidence?

PAUL MCGRADY Thank you. All right. I don't see any more hands in the queue. Oh, one more. Anil, go ahead.

ANIL KUMAR JAIN Thank you, Paul. One interesting thing which comes into my mind is that there may be a false alarm also when we select an associated domain investigation. For example, one website is hacked and after hacking that website, malicious activity is started on that particular website.

The possibility is that that gives a trigger to the community to start investigation. However, that domain owner, that registrant is not aware about this and he or she is struggling to get his website or domain to be out of this. I think we should exclude those compromised domains from the investigation for the associated domains. Thank you.

PAUL MCGRADY

Thank you. So, yeah, just to sort of restate that, the suggestion there was there's a difference between a bad guy registering a domain name for a bad reason versus an innocent person whose domain name has been compromised.

And Anil is suggesting that we do not need to do the investigation if it looks like the domain name is being used for DNS abuse, is, was, or might be, depending on where we land on that question. But if it's a compromised domain name, he's saying no investigation is necessary. So, we should write that down as a thing we think about.

We are going to -- Reg disappeared on me. She was in the queue. I'm sad now, Reg. Feodora, do you want to say something? You look like you wanted to. Jump the queue.

FEODORA HAMZA

I always want to say something. Sorry. What you just noted and I think Anil's comments, the Charter is very specific that compromised domains are outside of scope.

PAUL MCGRADY

Yeah, terrific.

FEODORA HAMZA

The Charter is very specific that compromised domain names are out of scope for this PDP. So just to confirm.

PAUL MCGRADY

So, I'm not doing a good job protecting the barriers of the universe if I can't remember exactly where all those barriers are. Okay, so compromised domain names out of scope and we shall never speak of them again. Terrific. One down and that made the other hands go away. Terrific. Okay, great.

So, looks to me, this has been a good discussion, right? So, it looks to me that we're not going to make this decision today, of course, but it looks to me like there are just a handful of options, right?

Is being used, is or and was, or is, was, and might be, right? And Brian or Reg is going to raise their hands and say, and Volker and Brian. Now I did it. I'm not saying I have a preference or that I think it should be one or the other. I'm just trying to capture what we talk about, right, so that we can see if we can congeal around the consensus on that. But because I triggered so many hands, I want to know what I said wrong. All right. So, we'll start with Reg. Reg, what did I say wrong?

REG LEVY

Reg Levy from Tucows. So. I guess my question to you would be, okay, we've had this conversation, but where are we, right? Are we answering this question? Because it doesn't seem to me like we have answered the question, and I'm not sure that it's reasonable to move on until we have the baseline answer that we at least

partially agree on, or maybe we're just here to chat. That's also fine. My understanding was we're here to answer the questions.

PAUL MCGRADY

We are absolutely here to answer the question. In my experience, what happens next is that from this comes a straw person recommendation with the different variations. We take a look at them when they're written down in writing, and we try to, through wordsmithing and otherwise, get to a conclusion about what recommendation we can get behind, right?

And so, if for example, after we go through that process, we can land at is only, then that's the consensus. If it's is and was, that's the consensus. If it's is, was, and might be, that's the consensus, right? But no, we're not going to draft that recommendation today, right? We didn't just chat. We sort of defined what the three options appear to be. Okay.

REG LEVY

Reg Levy from Tucows again. So just to respond to, or taking that in, thank you, who's drafting that straw proposal?

PAUL MCGRADY

Staff and I will draft it.

REG LEVY

I see. Thank you.

PAUL MCGRADY

Yeah, and that is what will come out on the list next from this conversation unless we still have more to say about this. I don't want to cut off communication, but question number two is a good one because it has nothing to do with is, was, or will be. It has to do with association, right? It's a different question that I don't think we need to have landed on question number one to jump into question number two.

We may run into questions like that that are definitionally dependent on each other and if we get there, then we'll pause, but that's the idea. That's why we have so much work in between calls to do, because we're going to be spending most of that time just eating up straw people and seeing if we can land. All right? All right. We have Volker, then Brian, then Jothan.

VOLKER GREIMANN

Thank you. Volker Greimann, RrSG, Team Internet, former nominee at CentralNic. I agree with Paul most of the way there. I think we don't have to have the answer before we can move on to the next one. I think we need to find a baseline first and just have a lot of discussions amongst the various points that we are discussing here before we can close one off.

I would prefer that the people that we are eating are made of something different than straw. I am not a cow, so different straw makes good burgers, but obviously, I don't want to turn into one.

But the point I wanted to make was, you might be wrong about the might be. I would prefer something raw more along the lines of has a high likelihood of becoming or above average likelihood of becoming. Might is too fluffy and lower threshold that I would feel comfortable with that. So, yeah, that's it.

PAUL MCGRADY

Perfect. I like that distinction. Otherwise, we're just in the realm of Tom Cruise movies, right? Yeah. So that's not great. All right. We have Brian and then Jothan.

BRIAN CIMBOLIC

Thanks, Paul. Brian Cimbolik for the registries. So, I liked your framing, but I think that it sort of the question of is, was, maybe almost gets more to, it's almost more agnostic than associated domain check and actually just gets into the question of mitigation of DNS abuse which I think is a little bit broader than where we are.

So, what I might suggest is that registrars are certainly within their rights if they want to, to act on mights or was, they're obligated to act on is. And so, I think that a place to start could be that upon action on a domain under 3.18.2 comma, that's when the associated domain check starts. And if a registrar chooses to only go with is, you know, that's the minimum, they must do that, then their associated domain checks would begin then.

If a registrar is more aggressive and says, okay, I found one name and it looks like it could be malicious, they're within their rights to

act on that domain. They wouldn't be required to, but still that would be a domain that they were acting on for DNS abuse to actionable evidence to their standard. So again, I think that it might be a good place to start that if we say upon mitigation of a domain under 3.18.2, associate domain check begins.

PAUL MCGRADY Does that capture was?

BRIAN CIMBOLIC It could, yes. So, this is my point, is that the registrar has the ability to go from as conservative to as aggressive as they want and the was would probably be somewhere in the middle. So a registrar could absolutely, and it sounds like Reg has, not to pick on you, but you specifically said it, has suspended a domain that isn't resolving content because it looks like it was engaged in DNS abuse. So, she made that determination and so that would still be a domain that was actioned upon under 3.18.2.

So, I think that's the point is that allows for some flexibility. It's the fact that the domain was actioned upon that I think is so important that that's where the launch point is. Now we need to roll up our sleeves and do homework and see if there's other associated domains.

PAUL MCGRADY Okay, Brian, that's a good advocacy for is. I'm not sure how it fits into was, but once we see it on paper, that's where the

wordsmithing in the Google doc comes down. Right? And maybe we don't end up at was, you know, I don't want to presuppose anything. Jothan.

JOTHAN FRAKES

Thank you, Paul. Yeah. Jothan Fakes speaking as a registrar with experience in this, but I'm here representing the SSAC. So, the might is a slippery slope and just to have the registrar hat on, it is expensive to get a customer. It is cheap to lose a customer. And so, there's a lot of care towards not doing friendly fire, misidentification.

But where there are some clear signals that might, I think if we have some heavier wording and I thought perhaps what was suggested in having heavier wording about the mights, perhaps in indications of clear evidence or otherwise, that we could pivot that into something that could be workable. Just so we're not going to accidentally cut down the wrong websites and affect customers, especially in the case of compromise. That's where the biggest sensitivity is in the registrar pool.

If you've got somebody who's already affected, you don't want to affect them even more because you're going to lose a customer really quickly. Not only are they affected and they're having problems in this other place, but gosh, you took down all their websites, that's not a good outcome.

But we do want to be able to -- if there's, you know, a pattern, like an entire branch of registrations, let's, you know, try and take out more than one. So, you want to have it flexible, but narrow in order to have the appropriate guardrails from doing too much especially under might, you know, because that's way too much flexibility. Thank you.

PAUL MCGRADY Thanks, Jothan. Yeah, and just to reconfirm, compromise is off the table, but point taken. All right. We have Gabriel and then Vivek. And I'm going to make wild claims that we might not get to question number two. We'll see. Vivek, go ahead. I'm sorry, Gabriel.

GABRIEL ANDREWS Thank you. Confused me there for a second. So, this is Gabriel Andrews for the record. And this is in response to one of the prior questions. Forgive me, I don't recall who it was that asked, but differentiating about, the difference between compromised domains versus those that are maliciously registered.

And before I raise this point, I want to acknowledge that the Charter would seem to make an exclusion of the compromised domains from the scope of this work. Nonetheless, there are some that are contributing to the GAC feedback that wanted to flag.

There may yet be occasions and circumstances in which a degree of associated domain check would still be valuable, even in the

case of compromise accounts, especially if there's the potential that other domains on that same account are also compromised as a result. And there might be opportunity to do such things as victim notification or harm prevention that would be flagged if one were to do associated domain checks in those circumstances. Over.

PAUL MCGRADY All right, Vivek.

VIVEK GOYAL Vivek for the BC. I'm mentioning this so that it goes in the straw and I understand the challenge behind it, but associate domain check could also help determine whether a complaint qualifies and becomes malicious enough for you to take action on. So, if we say that we will only do associate domain check once we have determined that the complaint is valid and we have taken action on, then we are losing an opportunity for a big signal that can help make that determination once a domain has been complained to the CPH. Thank you.

PAUL MCGRADY Thanks, Vivek. That's a new concept, right? So, we have is, was, highly likely indications and Vivek is suggesting that as part of the investigation of is or was to conduct the associated domain name check to see if it helps support the initial complaint. So that's something we hadn't talked about yet. So, we need to queue on that. Ching, go ahead.

CHING CHIAO

Thank you, Paul. Ching Chiao, BC. So, I'll maybe jump a little bit further. If I do, please hold me back, right? So, we're not talking really about how to, quote-unquote, clean up or, you know, suspend the name.

I think, at this question, we're talking about specifically whether this ADC name, sorry, the ADC name can be available, for example, in some way that maybe the third party will know that those are the ADCs. We're not talking about for registrars or registry to lose customers.

So, I think maybe ourselves, we're jumping a bit too much on this one. We're not talking about once this is an ADC and then you should take or you should put a server hold on all the names. I think as of now, the goal is to see because some of the information that's held by the registrar won't actually not be available publicly.

So that's where the ADC is much needed for certain part of the community, whether it's a law enforcement or from the cybersecurity vendor. If that list is available for some of them to take early action, that's something we, I mean, could help. Once again, we're not talking about, hey, if this is ADC, take them all down. No.

PAUL MCGRADY

Yeah, so because you asked me too, Ching, I will say like that's way outside the universe, right? We're not talking about what happens

next, but, you know, again, good to hear that there would be some use for that and maybe that goes into our ideas that we feed back to counsel. But you know, that's outside of our universe.

Reg, I hope you're going to talk about inbound, yeah, to Vivek's point, that if you get an inbound complaint about an is being used, right, Vivek is suggesting that that should trigger the investigation into associated domains. And so, react to that, please, if you don't mind, and then whatever you wanted to say. Thanks.

REG LEVY

Reg Levy from Tucows, and I would submit that what I was going to say is a reaction to that. I've dropped it into the chat, but a number of us have been doing some homework extracurricularly, unassigned, and have presented a straw proposal as follows.

When a registrar takes action under Section 3.8 of the Registrar Accreditation Agreement, the registrar shall promptly review other domains that are reasonably associated with that domain when there are clear indicators that other domains registered by the same customer may be involved in the same abusive activity, using information reasonably available to the registrar at the time of review, and take action against these domains where appropriate. And thank you very much for whoever's putting that on the screen right now.

So, I think that this covers the is in as much as I understand exactly how that verb is being used. That when there is abuse found, we

take action or rather, when we take action, then this triggers the policy that is being proposed. I know that people are going to need some time to think about it, but this is something, like I said, that we've been workshopping in the last couple days. I'm sure it can use some tweaking and we look forward to input.

PAUL MCGRADY

Thanks, Reg, and this is actually super helpful, right? And I encourage anybody else around the table to go ahead and look at the Charter questions. And this is to Volker's point, look at the Charter questions. And if you have proposals like this about what you think it should be or what your group can bring to the table on this to think about it, go ahead and let's start letting those fly because that's going to help speed this up. So, Reg, thank you for that. That gives us something concrete.

And, you know, I understand it reflects the is, not the was, or not the highly likely, but it's a great starting point. Go ahead.

REG LEVY

It actually does address the was or the highly likely because it depends on the determination made by the registrar. Because in some cases, registrars will take action under 3.18 in the circumstance of a was or a may. So, it's not the is necessarily, it's the action that was taken.

PAUL MCGRADY: But that action could have been taken by not registrar, could have been taken by the host?

REG LEVY: So, where an action is taken by the registrar, it triggers this. If the action was taken by the host and the registrar reviews the action taken by the host and takes their own action, that triggers this. So that's the was that occurred. So if the registrar takes a look and says action was taken somewhere, but we don't actually see any ongoing evidence and takes no action, then no, this would not be triggered. So, it matters what the registrar reasonably does under 3.18 and in some cases that will include the was or the might.

PAUL MCGRADY: Thank you, Reg. Gives us something to work with. I like concrete things. We have Brian Volker and then Luke. I think that will take us to time, but before we hear from Brian, I'm going to suggest something to you all.

As we have heard throughout the community this week, everybody wants us to really beat our timeline. And so, I want everybody to do a little personal homework to think about ways we can do that and if we have the emotional and physical and intellectual will to do that.

And I would love for us in one of our future calls, not very far from here, to take a look at our work plan and see if we can accelerate it in some ways without giving ourselves an unreasonable deadline.

Because we could be one of the fastest PDPs of all time, but miss our deadline by a week, and then we're in the doghouse, right?

So, everybody think through our timeline. We'll take some chat about that on our next not here call. All right, let's round out the time with Brian, Volker. Actually, I'm going to do something.

Since we've heard from Brian and Volker a lot, we're going to put Luke up front because we could very easily run out of time and I'm going to end in four minutes. Okay, so Luke, go ahead.

LUKE WOOD

Thank you. So, Luke here from Netcraft on behalf of the BC as a member, so initial first great straw poll RS3 my initial statement is on the associated customer. So the campaigns that NetBeacon and similar entities in the vendor space like Netcraft, we often say huge campaigns associated with phishing as a service typically those campaigns are under different registrants and different customers.

So, if you're looking at the same customer, you might just find four domains. But if you look at the entire campaign, it goes back to the second question we've not had time to explore, you actually see there's a huge campaign, even not mitigated, because you've only looked at one customer. Just sharing the observation. Thank you.

PAUL MCGRADY

Thank you, Luke. All right. We have Brian and then Volker, if we have time, Volker.

BRIAN CIMBOLIC Thanks, Paul. I'll try to be quick. Brian, for the registries. I just want to point to something that Jordan and I were both pointing out in the chat. Really, the way I view the Charter, and boy, I think maybe it'd be good before each meeting, we all just, let's take a skim of the Charter. And I think that was, might be, or anything other than is may potentially really be out of scope for the charter.

Because it says the PDP seeks to create an obligation for registrars to investigate other domains associated with a customer account or registrant where at least one domain of that registrant is found to be engaged in DNS abuse as defined in the RAA. There's a couple other points in the Charter where it really does point to upon confirmation, upon mitigation, that is when the registrar, we're trying to create the obligation to look, to pivot onto the other potential associated domains after the is.

PAUL MCGRADY Thanks, Brian. All right, we have Volker.

VOLKER GREIMANN Yeah, just very shortly in response to Vivek, doing it for every abuse complaint we receive is highly uneconomical from a time management perspective because we would be running donuts around, making investigations where there is no likelihood of finding anything. And therefore, we would probably waste time that we could be spending in actioning other reports.

I think it's very important that we focus this on cases where we have a likelihood of finding something as well instead of just going through the motions, acting and doing a shadow play acting and fulfilling certain, crossing the T's, dotting the I's and not doing any productive work in that time. Thank you.

PAUL MCGRADY All right. Thank you. We are going to go ahead and call it. Vivek, I saw you. Well, I'll give you 30 seconds. Go ahead.

VIVEK GOYAL I understand not doing it for everyone is not my recommendation at all. I know it's a waste of time and I wouldn't do it if I was in your position. My point was that I know that many registrars currently do this already as a practice, but the reason why we are here is to force the people who don't do it to force them to do it. So if it is a good practice, which deals benefit, how can we build it into the policy so the lying registrars who lie all the time can also use this and maybe their lying reduces? That's my hope. Never asking for everything to be changed. Thank you.

PAUL MCGRADY All right. We did it. Thank you, everybody. Good conversation. We will distill all this down. Remember that if you have specific language you want to be considered, it is the opposite of bad behavior. It's good behavior to put it forward. Thank you, Reg. And I wish you guys all safe travels and thank you for your participation.

ANDREW CHEN Thank you, everybody. Please stop the recording.

**[END OF TRANSCRIPTION]**