
ICANN84 | AGM – GNSO: DNS Abuse Work Session
Sunday, October 26, 2025 – 10:30 to 12:00 IST

TERRI AGNEW:

Hello and welcome to the DNS Abuse Work Session.

Please note that this session is being recorded and governed by the ICANN community participant code of conduct, ICANN expected standards of behavior, and the ICANN community antiharassment policy.

Please observe the following guidelines to participate in the session. I will also post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during the session as time permits when directed by the chair of the 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 back over to Jennifer Chung. Please begin.

JENNIFER CHUNG:

Thank you, Terri. This is a very small room with very few attendants. No, just kidding. I think this is quite an interesting topic for everyone, so we're all here. My name is Jennifer Chung. I am just a person that is here to facilitate this very important discussion. Welcome to the session on DNS Abuse. Thank you all for joining, of

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file but should not be treated as an authoritative record.

course, and your continued engagement on this very important topic.

As you know, the Preliminary Issue Report on a PDP on DNS Abuse Mitigation was published following the Council's request on 14 August this year. The report builds on the work of the DNS Abuse Small Team that was convened earlier this year to assess new data, research, and community input, particularly in the light of the strengthened RA and RAA provisions that took effect in April last year.

The small team's analysis focused primarily on issue identification and scoping. From its review three potential areas for further work were highlighted, and two of those—unrestricted API access for high-volume registrations and associated domain checks—were identified by preliminary issue report for inclusion in the scope of a narrowly focused PDP.

Today's session aims to take this discussion a step further. While the issue report and the small team were concentrated on defining and framing the issues, our goal now is to begin exploring potential solutions, outcomes, and to think about how these issues might be addressed through future and potential policy work and development. Specifically here, we really want to gather community perspectives on possible ways that these issues might be addressed, including what policy requirements can be effective and also collect input and reflections that can serve as food for

thought both for the draft charter which is really important and for any updates of the issue report before it's finalized.

So it's really worth noting now holding a dedicated community session here in—and really few attendants around this room. No chairs are being sat on. This is really important because this is not actually standard practice after a preliminary issue report. But because this is such an important issue for the ICANN community, DNS abuse mitigation is one of the top topics for really all across the board here, we felt it was really valuable to create this additional space especially as we're meeting here in Dublin. And early alignment on the expectations for the potential PDP is really, really important.

So to help trigger food for thought and to spark conversation and discussion, we'll also be using a few short survey questions on Zoom. So everybody in the room please do log into the Zoom link, otherwise we won't be able to get the temperature of the room. Please do that. These questions are really designed to just gauge the temperature of the room, to understand different perspectives, and to help identify areas of convergence and divergence of views.

There are no right or wrong answers. All responses are anonymous and nonbinding. The purpose is really not to make a decision today but to allow everyone, and of course the entire community, to start reflecting on how these issues might be addressed in practice. We look forward to an open and constructive discussion today, and your input will help inform our final issue report and provide useful

context for the GNSO Council's consideration on next steps on DNS abuse mitigation.

Thank you again, and I think now I'm passing it over to Steve.

STEVE CHAN:

Thanks very much, Jen. One of the most important questions in how to set up this work is really about setting up the charter and a big part of that is making sure we understand what topics should be addressed in that charter. So that's why you have this segment here that concentrates on the structure of the PDP. And so there was quite a bit of public comment received to the plenary issue report. There were 27 comments, which is really great engagement. So we're still working through the public comment analysis, but from what we see there are a lot of comments about the structure of the PDP and what people think should be included or not included and whether or not they should be combined in a single PDP or separated.

And so what we want to make sure is that we provide some clarity about the nuances of what it meant to have a PDP with two topics, and that's not quite a binary black and white thing. So it's really going to end up on the Council's decision-making to determine how the structure should look, but we want to make sure that there's good information to be able to make that decision.

So just by way of getting into the details of those comments, I think it's fair to say most of the commenters expressed some concerns

about a single PDP covering multiple topics and expressed some concerns that might make the work inefficient and overcomplicate the process. And so, like I said, that's why we want to make sure we provide a little bit of clarity and nuance about what it means either to have a single PDP with two topics or to have two PDPs with individual topics.

So with that, we have a couple of slides. I won't go into too much detail because we have pictures instead. In blue here...like I said I'm not going to go into detail. I think the picture will make it easier to understand. So there are essentially two options when you talk about a PDP. A single PDP with two topics. And the next slide. And then there are essentially two options when you talk about two PDPs, individual ones each with an individual topic.

So the pictures. And I am very poor at making slides, so apologies. This is me. They're not good. They're color coded. I don't know why everyone is still laughing. It's kind of rude at this point.

There are two in blue. These reflect one PDP with two topics. So what it reflects, and I think this is the concern of many of the commenters, is that you have to solve two issues before either of them come out of the Council and go toward implementation. And so that's what Line 1 represents. It shows that you initiate a PDP that includes two topics. You have to solve and develop recommendations for both the topics. It leads to a single initial report, a single final report. And it's not shown on the graphic here, but then through Board consideration and implementation and

ultimately policy effective date. So I think that is the one that mostly commenters are most concerned about is Line 1.

And so the nuance I talk about is essentially the second line. This is still a single PDP with two topics, but essentially you're having them conducted in what we call phases. It has been used in other contexts for the IDNs EPDP that operate in phases. And so what you have here is you essentially take the first topic. You take it through the initial report, final report, to the Board and implementation for a single topic and then you tackle the second issue.

And so what it allows you to do is to take the wins, essentially, from that first topic and have it go through its merry path to implementation. And what it does is essentially it reduces some of that administrative overhead of having to initiate a PDP and having to initiate another PDP after that. So it's just functionally I think from the staff perspective it's not that much different from having two PDPs that take place in succession. So that's essentially what we call a phased PDP with two topics. Next slide, please.

This is the structure when you have multiple PDPs. This is Example 3. There's probably little nuance here but essentially what this shows is a single PDP with one topic. You go through all the processes included the reports, Council consideration, and then Board consideration and implementation. And then you initiate the second PDP and do all those different things which, if do them end-to-end, can take quite some time. And so the nuance here I think is you don't necessarily need to wait to start the second PDP after

everything is completed from the first one. You could have them overlap. That's a little bit of nuance here.

And then the last slide is just the one that honestly scares staff from a researching perspective. It's having two PDPs run completely in parallel because you essentially double all of the resources both from the staff side but also from the community as well.

And so like I said, we just wanted to make sure that there's clarity on what it means to have a single PDP with two topics, that there is still a way to pull out the outcomes from that first topic, have it go through all of its processes through the Board and through implementation, and essentially it doesn't look that different from Example 2 versus Example 3 in reality.

I think that's almost it. Yeah, sure, I'll take a question while I [inaudible] supposed to say.

CHRIS DISSPAIN:

The concern I have of your, is it Slide 2? Can we...? Yeah. No, sorry. The one that has the...anyway, whatever. The one that you said had the one PDP but you don't start the second PDP until you finish the first bit. That assumes you're going to have the same people, and I think that's a real challenge because I actually think these topics may well invite different members of the community to be representatives of the GNSO's stakeholder groups on those topics, especially in respect to technical expertise and stuff like that. So I

think the challenge you have with that is that you're going to end up with one...if you're trying to do one PDP.

So really the only difference between your suggested, leaving aside my point about the different people, the only thing that it causes...it shouldn't cause you any logistical problems other than the fact that you're right when you say you'd need to charter a second PDP. But I think you can solve that problem by writing both charters now, setting both charters in stone right now and then saying we're going to launch this one now and then as soon as that final report is finished we're going to launch the second one. You could even have the people lined up. It doesn't stop you from doing that. So I don't actually think there really is a logistical challenge for your. And I think from our side of things really we need that flexibility of putting different people on the two PDPs. Thanks.

STEVE CHAN:

Thanks very much, Chris. I think an important point to make here is that all you're seeing here is some staff suggestions on how to structure things. The decision ultimately rests with the Council. So if they hate our idea and they like your idea, that's perfectly fine with us.

Is there anything else I wanted to say? Actually, just one other last point is that—and I'm not sure if Russ is in the room and I hope he doesn't kill me—but one of the things that we are expecting to do is provide a little bit more resources to this PDP than you would normally expect. So a typical PDP would have weekly meetings.

That's the typical cadence. You meet online and you meet at ICANN meetings. And I think what we envisioned for this PDP is because it's such an important topic to so many in the community is allocating extra resources. What that means in reality is likely a face-to-face for the working group. So that is potentially a consideration. So if you want to have that face-to-face only on a single topic, that might be a result if you have a PDP with a single topic. If you have it with two, you potentially have an ability to tackle two in that face-to-face environment.

CHRIS DISSPAIN:

Not on the cadence that you put up because you didn't start the second one until you finish the final report on the first one. So that can't apply to what you put up as your suggested cadence. Thanks.

STEVE CHAN:

I think that's a consideration. Yeah, I'm done. Queue away.

JENNIFER CHUNG:

I see there is a queue building. I think we had a slide with questions to stimulate some discussion and thought, but I think there are a lot of thoughts and questions already. So let's go straight to the queue. We want to hear from everyone. Susan?

SUSAN CHALMERS:

Thank you. Susan Chalmers, GAC representative for the United States. Thank you so much for the presentation. Just a question for

clarification. And forgive me if you covered this. I just did not see it indicated on the slide. Where does implementation fit in, in these two paths? We see the PDP and then the final reports, but we just have a question about where the implementation would fit it.

STEVE CHAN:

Thanks, Susan. Yeah, it stops at the final report, as you're ICG. So the step after the final report is delivered, it goes to the GNSO Council and the GNSO Council gets to consider and vote on the final report. Then it goes to the Board for the consideration of the recommendations from the GNSO. And if they adopt the recommendations, then it goes to implementation.

SUSAN CHALMERS:

It might be helpful to illustrate that as well. It's unclear whether or not implementation on a first PDP, for example, could be moving contemporaneously with the initiation of the PDP on the second topic. So just a suggestion. Thanks.

JENNIFER CHUNG:

Thanks, Susan. We'll go to the next in the queue. Thomas?

[THOMAS]:

Yeah, thanks so much. And first of all, Steve, thank you so much for boosting my confidence in my own PowerPoint skills. That's been very helpful. I was thinking that maybe we have to play a little bit of 3D chess here. Why not let the two PDPs run, and I was hoping

that you could bring up the snake chart that we typically use when we're looking at PDPs. Because that has the implementation part in it and it has all the public comment periods in it. I think that maybe one of the PDPs gets to a solution faster than the other and then when one goes to public comment, in those 40 days or something the other PDP can put more efforts into advancing the topic.

I think that actually we're going to end up with hugely congruent teams that work on both topics. I don't think that they're completely distinct from each other looking at the usual suspects that typically show up at these meetings. So maybe we can use the public comment period and focus more on one than the other so that we can declare victory on one of them, and we don't know which one, easier. There might be delays for one while the other might go faster, so I would be very much in favor of exploring letting them both run at the same time and see who is going to make the race first.

And then also we have more topics than the two. That would give us the flexibility when one is thrown over the fence to the board that we then or maybe even a little bit earlier initiate the next topic so that we move as fast as we can. Thank you.

JENNIFER CHUNG:

Thank you, Thomas. And thank you, staff, for putting up the Z process. I think everybody hopefully in this room has seen this before. If not, please feast your eyes on this beautiful Z diagram

made by Steve who is very good at diagrams but can improve on PowerPoint. Let's go to the next one on the queue. I'm not sure who this is in India. Please go ahead.

UNIDENTIFIED MALE:

Yeah, I'm here. I think the expectation is that this PDP process will be completed before the next gTLD round. If that is the expectation, then I think I would second what Thomas said just before me that we may start the two processes [in back end]. And also, I think in this computer age who works in a serial fashion? No one works, right? So it would be really kind of shocking in case we start to take a serial process approach and one stakeholder or the one process blocks the complete PDP or [inaudible] the PDP. So it would be better if we allocate more resources which shouldn't be a challenge. I think there will be more people, stakeholders coming forward, those who have interest in this. So I would propose that we should follow the Option 4 that starts the two PDP processes in parallel. Thank you.

JENNIFER CHUNG:

Thank you. I think the short answer is there is no expectation for this to compete before the next round, but staff can add color if they would like to.

STEVE CHAN:

Thanks. I would just note there's maybe a little bit of nuance. There's the start of the round, and then there's another milestone

which is a natural one which is delegation. So the start of the round is logistically impossible. Delegation has a possibility. Thanks.

JENNIFER CHUNG: Thanks, Steve. Nick, please go ahead.

NICK WENBAN-SMITH: Thanks, Jen. It's Nick Wenban-Smith, Nominet.uk. I chair the ccNSO's DNS Abuse Standing Committee, so I'm interested in this topic, obviously. But I'm not here to preach to the GNSO as to how to do their PDPs particularly. So I pray on my paternal grandmother who's Irish and speak in the local vernacular. I think both of these PDPs are what's known in local terms as "bleeding" obvious and pretty simple and straightforward. And you should be ambitious and maybe make it a competitive tension to start them both and see which one can finish first. Because I think there's a danger here of overthinking it through all of your various processes, and I think that the results are really tangible and important and should be progressed really urgently and quickly as possible.

JENNIFER CHUNG: Thanks, Nick. It's always good to see practices from the ccNSO. GNSO can also take a look at it and learn from it. I think we're going to be putting up some poll questions on the Zoom room. So a reminder for everybody who is in the room. Please log on to the Zoom room for this session because there will be a poll. There you

go. And as that is being answered, I think I can go to the next person in the queue. Margie Milam?

MARGIE MILAM:

Hello. I'm Margie Milam, and I'm representing the IPC in this capacity. As we put together our comments for the initial report we certainly see the need for improvements and to be done very quickly. Our concern is the timing. If you look at the slide deck, you can see that it's going to be years before anything actually gets implemented. And in our view, that's a problem. We appreciate the product approach and we just want to suggest that where some of the work maybe, like Nick said, obviously should be done, is there a faster way to do it? Can it be done through contact negotiations? We saw the great work that the registrars and the ICANN staff did in coming together with the first round of negotiated topics. Is there a way to do that as opposed to going through this very long process? Because while we wait, the abuse continues and ICANN has a lot on its plate. If something is obvious, let's see if there's an easier way to do it.

And the second point I'd like to make is that this is only talking about two topics, but there are a lot of other gaps that need to be addressed and in our view it's just not acceptable to wait three, four, five years to get to those other points. A classic example of that is the definition of DNS abuse. That's not one of the PDP topics yet that is something that I think needs to be, or at least from the IPC perspective, needs to be looked at taking into account some of

the recommendations that the SSAC had made in their prior papers.

So I know that the PDP report was focusing specifically just on the processes, but let's be creative here and see if we can come up with alternative ways of doing this such as the community perhaps coming up with negotiation topics for amendments to the contract that address these points as opposed to going through this lengthy process. Thank you.

JENNIFER CHUNG:

Just a reminder for all of us as well in the preliminary report I think we also had Recommendation 4 that does very substantially and comprehensively list out a lot of the topics that the SOs, ACs, SGs, and ACs have indicated are also very priority topics. So rest assured these are not going to go into a black hole or a black box or anything like that. It's noted and it is also important for the community to consider after we look at the priority topics here.

I think we have some answers to the poll. Maybe staff would be happy to show on screen. Oh, okay. Do we know how many responded? That's quite a lot of response, 83. That's very nice. It looks like there is a large part of us who think separate PDPs for each topic is the way to go. The next one in a little bit there is a single PDP covering both topics. Am I reading this right? Yes. Maybe I should look at my own screen. That is right. Instead of trying to squint at the screen. I don't see it on the Zoom.

UNIDENTIFIED MALE: It's not there.

JENNIFER CHUNG: Okay, and then there's a portion of us who look at the single PDP with a clear phased approach from the start, and then there's "other." I wonder who the others are. Maybe they're already speaking.

Let's go back to the queue. Susan?

SUSAN CHALMERS: Thank you. And I should have prefaced my first intervention with a little bit of housekeeping. I serve as one of the topic co-leads in the GAC on DNS abuse. There are three topic co-leads. I work with colleagues from the European Commission as well as Japan on this issue. And then I'm also joined by my colleague Janos who is from the PSWG today.

We did want to mention that on timing the GAC did lodge a submission and also in our ICANN83 advice we do wish to see PDPs completed in advance before the DNS is expanded for the next round, by the next round.

In terms of process in our submission, really it's just a matter of which path will get us there fastest. So we're just looking for the most efficient approach.

And in terms of the structure of the PDPs, we'll be looking forward to hearing what the community thinks here but the poll is very helpful. Thank you.

JENNIFER CHUNG:

Thank you, Susan. And thank you, GAC leads, on DNS abuse have been engaging on the whole topic. Next in the queue...oh, before I go to the next in the queue I'm noting that we're closing the queue on this topic after Farzaneh. Michaela?

MICHAELA SHAPIRO:

Thank you so much. Michaela Shapiro, Article 19 representing the Noncommercial Stakeholder Group today. I just wanted to offer a few thoughts on the different options that have been presented.

First, just to note that for the Noncommercial Stakeholder Group the option of having two parallel policy development processes would be extremely taxing on our limited resources and capacity. We would also want to note that with each of these two different policy development processes there are different safeguards that we would want to have considered in each of those that we wouldn't want to have rushed.

So if we were to move forward with any of these options, we would also have some recommendations for the kind of questions that we would want to include in the charter. We would highly encourage having separate charters regardless of whether they're in parallel or perpendicular, however they fit together in terms of the timeline

and would be happy to offer more concrete recommendations on questions that could be added to any of the charters.

I think those were the main points. Thank you.

JENNIFER CHUNG: Thank you, Michaela. I hear both from the GAC about efficiency of timeline and I hear from NCSG things should be considered in a way that does contemplate questions. I assume you are pointing toward the human rights impact assessment?

MICHAELA SHAPIRO: Yes, and I would say just that there are certain safeguards that would be, yeah, human rights safeguards that would have to be included in either.

JENNIFER CHUNG: Thank you, Michaela. Justine?

JUSTINE CHEW: Thanks, Jen. This is Justine Chew from the ALAC. Just a couple of points about the public comment that we put in. The ALAC is in a position of doing as much as possible for DNS abuse I think similar to what Margie said, but we accept the fact that we're just going to concentrate on the first two that have been identified. And we would like to see speedy progress on this as well.

We took the position or the approach to putting some preliminary questions for the charter in our comment. So we have gone one step ahead. Hopefully, that's useful for Council's consideration when they look at actually initiating the PDP.

But my question is regardless of whether we take the parallel approach or the sequential approach, I'd like to get some indication maybe from our contracted parties colleagues here on this question that's on the board which is the third one. Whether we think that either one of those gaps would be easier to resolve than the other. Thank you.

JENNIFER CHUNG:

Thanks, Justine. We closed the queue, but I'll let CPH colleagues have a quick response if they do have one. Farzi, is it okay for them to have a response first? Thank you, Farzi.

REG LEVY:

Thank you, Farzaneh. So I first want to clarify that there are three issues up. And while the staff report indicated only two, the comments seem to ICG that the entire community is interested in all three. So I will speak about three generally or PDPs generally.

I think that the associated domain check is going to be reasonably easy to attain registrar consensus on, and my understanding from the registries is that the DGA is relatively noncontroversial. So either of those two I think could go forward first.

BRIAN CIMBOLIC:

Thanks. From a registry perspective I agree with Reg. I think that the associated domain check to me I think is the most impactful because it gets directly to one of the issues that we've been hearing about and that's bulk registrations. And it helps address that problem without getting into the weeds and trying to define what "bulk" is. So I really do think the associated domain check has the opportunity to be the most impactful.

Reg correctly points out that there were three areas. There's associated domain check, friction in APIs, and DGAs. And so the registries are certainly supportive of community work on DGAs whether that's a PDP or other mechanism. The only issue I did want to point out is that DGAs sort of necessarily span both gTLDs and ccTLDs, and so we just want to be careful that whatever solution we build to help address that problem we have sufficient participation and representation from our ccTLD friends.

That is a solution that would get used. Just the Avalanche botnet very famously the most recent big one in the first year had 832,000 domains associated with it across 60 TLDs in 57 jurisdictions. So that's the sort of scale you're dealing with, so we need to just be careful that whatever solution the community comes to on DGAs doesn't end up being only a gTLD issue.

JUSTINE CHEW:

Thank you very much for that input, Reg and Brian. Very helpful.

JENNIFER CHUNG: Thank you. I see some hands up. I'm assuming there are legacy hands there, but I will now go to Farzaneh.

FARZANEH BADIEI: I'm a member of NCSG and also on GNSO Council. We are in favor of...whatever format that we have we are resource constrained. And logistically most of us don't get paid. We cannot allocate budget for participation in these PDPs. So if it can be less resource intensive to have both topics in one PDP but phased, we do not want anything to happen in parallel, that could be an option as well.

And on associated domain checks, NCSG has withdrawn its support for—not that it's going to make any difference—but we want to record that we have withdrawn our support on working on associated domain checks before the human rights risks are established because we believe that there might be a lot of risk in associated domain checks and how we do it. It can lead to profiling people and domain name registrants. Thank you.

UNIDENTIFIED FEMALE: I'm sorry. I want to say something. Can everybody in the room log into the Zoom? Because we are taking polls and stuff. Yeah, we want to hear you.

JENNIFER CHUNG:

Thanks, Farzi. Steve had his hand up. Steve?

STEVE CHAN:

Thanks, Jen. Just a really quick comment. This is Steve again. I just wanted to thank everyone for their input because as Jen mentioned this is not typical. We don't do a plenary issue report and have a public session like this. So it's just very valuable input. We still have the task of revising the issue report, revising the draft charter that's included, and all of this helps us make sure that it's in a better place for the Council. Thank you, everyone.

JENNIFER CHUNG:

Thank you, Steve. And I think we are going to the next topic which is not the format of our very first one, access to API. I'm going to throw this over to Feodora.

FEODORA HAMZA:

Thank you, everyone. Let us know turn to the first issue identified in the preliminary issue report. This is just a brief intro before we go into discussion.

Unrestricted API access for high-volume registration has emerged as one of the priority gaps in the DNS Abuse Small Team report from this year. The report found that while many registrars use API or batch registration tools to enable customers to register domains efficiently, unrestricted or ungated access to these tools can unintentionally facilitate DNS abuse, sometimes at large scale.

So according to some studies, including also the ICANN commissioned INFERMAL studies, registrars that provided unrestricted automated API registration capabilities experienced a significantly higher incidence of malicious registrations.

So now the aim of addressing this issue within the PDP is not to restrict legitimate business models or automation but rather to explore appropriate safeguards that can help prevent the high-volume registration of domains for malicious use. So the discussion is therefore about balance, ensuring that operational efficiency and innovation can continue while reducing the potential for systemic or organized or high-volume DNS abuse in this case.

What we would like to hear from the community is what do you think? Did we scope the issue correctly? Are there any potential solutions to this you can already share with us? And are there any charter questions that we should consider in addition to it?

So, Jen, back to you.

JENNIFER CHUNG:

Thank you, Feodora. I see the queue starting already. Can we go to the next slide for some questions that will trigger some discussion? And also, I think we're going to launch the Zoom poll, so those in the room who just came in please be in the Zoom room so you can answer the Zoom poll.

I'm going to go straight to the queue because I see a queue forming.

GREG AARON:

Hi. I'm here monitoring the work here on behalf of SSAC, but I'll just speak as a professional in the security world. When the small team started talking about this topic, it called it "bulk" registration. And then later the language has shifted to emphasizing APIs. It will be important to scope and define the problem you're trying to solve.

I think a lot of the people who have been commenting on this are saying the problem you need to solve is that bad actors go get lots of domain names. APIs are one way they do that but not the only one. And if you focus exclusively on APIs, you may not solve the problem that you set out to solve.

For example, you can go to a registrar site and just use the website and web tools. They're not actually as a registrant interacting with APIs at all. So scoping will be important and we'll have to figure out the problem you're trying to solve. API access only might leave a lot of things off the table and might not solve the problem.

JENNIFER CHUNG:

Thanks, Greg. Maybe just a small follow-up question because we are trying to have a very focused PDP able to answer a question, be able to get to implementation. Your reminder, which is very important from a security point of view, but is this a consideration for us to look at our charter? Is this a consideration for us to look at the fourth recommendation of additional buckets of items that are also very important to solve?

GREG AARON:

Yeah, I don't think it...this is actually a discussion of what's out of scope. I think the problem was defined. But if you just say APIs, that's very restrictive. I think what we're probably talking about is how do we allow access so people can get large batches of domains, and part of that issue is who do you decide is qualified or who shouldn't get it? So I don't think we're out of scope talking about bulk registrations. APIs are an important part of it, but the emphasis in the language has changed and it actually could be material.

JENNIFER CHUNG:

Thanks, Greg. I can't read this. Janos, please go ahead.

JANOS DRIENYOVSKI:

Thank you. I'm co-chair of the Public Safety Working Group. I would need to start my intervention with a small disclaimer as any viewpoints expressed by me here are offered with the understanding that none of this is from the PSWG position but rather is reflective at this stage of member discussions as we consider these new policy development proposals which the PSWG supports and as good next steps for DNS abuse mitigation.

With that said, I just wanted to first react on the first question and provide some input as the PSWG believes that the proposed examples in the question are good to explore. So the waiting periods between transaction history abuse checks are good

avenues to pursue. We would also add organization identity checks could be helpful as APIs are most likely to be used by organizations and not individuals. And checks concerning organization details should be very visible and not infringing on [inaudible] requirements.

So perhaps exploring the idea of getting [inaudible] capabilities to new customers only after organizational identity checks would be a worthwhile thing to explore. I will stop there for now, and I might take the floor on the other questions depending how you plan to proceed. Just reacting on the scoping. And I believe that the concept here is to have a focused PDP, so I'm trying to understand how material impact would this language change mean exactly. But to us it doesn't seem to debate too much on what the advice set out to do, the scope. Thank you.

JENNIFER CHUNG:

Thank you, Janos. PSWG input is always very important for us to consider as well. Sorry for not being to attempt to speak your last name. I will do better. Catherine?

CATHERINE PALETTA:

Thanks. This is Catherine Paletta from Identity Digital. I'm not technically on the dais but I saw a roving mic and I thought I could raise my hand. And then I came to the table for this one instead. I just wanted to speak to the poll questions. Did I say I'm from the Registries Stakeholder Group? That's where I'm from.

I'm a little concerned about these poll questions which seem to going to the outcome of the PDP which is not something for this group to decide. That's for the working group of the PDP to decide. I think the community should be on board with a narrowly scoped PDP that is able to consider all, any outcomes, including these and including ones not listed here. So I'm just a little concerned that we're getting into talking about solutions and it's too early for that kind of discussion. Thanks.

JENNIFER CHUNG:

Thanks, Catherine. Appreciate that. And just before I go to Feodora who will give us some color into why the poll questions are the way they are, a reminder for the entire room. This is not just for people sitting at the U-table. It's for all of us, and there is a roving mic. If you don't see the roving mic, I think Seth can give you a roving mic if you put your hand up in Zoom or you can come to the table like Catherine. But now I'm going to give it to Feo to add some color.

FEODORA HAMZA:

Thank you. I just wanted to remind the room and the group that like Jen said earlier that these questions are just here to help us update the issue report or the draft charter. It's not going to be the ultimate solution. It's just to understand what is possible and could be an outcome so we can scope and frame accordingly. Of course, as said earlier, these answers and questions are not binding, and we also appreciate if there is anything other than we've mentioned there. So we would like to hear from you as sometimes our assessment

doesn't encompass everything. So that's why we're having this session to hear from the community. Back to you, Jen.

JENNIFER CHUNG:

Thanks, Feo. Just checking in with Catherine and others who had the same query in their head if that's answered. I see a nod. That's great. Back to the queue. Greg Aaron? No, that's an old hand. So now Michaela.

MICHAELA SHAPIRO:

Hi. We just wanted to concur from the perspective of the Noncommercial Stakeholder Group with Catherine's comments. We also just felt like it was a tad preemptive at the moment but appreciate what you're trying to do here. So thank you for the offer. Just commenting on some of the specifics of the questions, I think from the Noncommercial side or at least speaking from Article 19's perspective the terminology used in terms of safeguards I think we would interpret slightly differently. I think we would normally use that terminology when referring to human rights safeguards whether it's a privacy protection, surveillance protection, data protection, kind of perspective. So there are certain safeguards that we certainly would want to have in there, and I think it would be important for the PDP to consider what those safeguards would be. That applies also for Question 2 in terms of what those different elements would be.

I think we would just want to push back initially just already on the—there was one specific one that I just wanted—on activity based trust squaring just to say from Article 19’s perspective and the NCSG would concur that behavioral indicators are not an area that we would typically be supportive of.

And lastly, similarly on the last question in terms of we could potentially be behind some kind of either temporary restriction or warning. We would just want to ensure that there is clear and consistent and coherent communication with the registrant when that were to happen. But again, I think we’re putting the cart before the horse a little bit at the moment but wanted to put that on the record. Thank you.

JENNIFER CHUNG:

Thanks, Michaela. That’s very useful. I think this is also a good exercise actually for us to get the charter questions right, to frame it right, and for all of the community to tell us specifically on certain terminology we need to be more precise and articulate. We're going to go through, before we go back to the queue—oh, the queue has changed. Yeah, we’ll go to the queue and then we’ll look at the answers to the poll. So, Ann, please go ahead.

ANNE AIKMAN-SCALESE:

Thanks, Jen. Anne Aikman-Scalese on Council as NomCom, nonvoting, fully retired, not representing any particular interest other than organizational effectiveness, I would hope. And I want

to agree with Jen's observation that these poll questions are actually quite helpful to composing a proper charter, framing issues correctly, using correct language. And I think that getting thoughts at an ICANN meeting in an open way in this fashion is super for our transparency reputation as well and very good for ICANN. And I want to thank you for doing the polls. Thanks.

JENNIFER CHUNG:

Thank you, Anne. And kudos also to the staff team who has been very supportive with all of the transparency and openness and particularly for the Council small team on DNS abuse. We made all the small team working calls open for all observers, so I think this is a very important topic and we note that.

Let's take a quick look at the responses. I don't know why it doesn't show on my screen. I'm going to either squint. I will squint. Okay, in your view, how important is it to apply minimum safeguards before granting high-volume or API access to new accounts? There is a—oh, thank you for expanding that—there is quite a large percentage, 71% says it's very important. We have 15% saying somewhat, 7% with neutral, 6% not very important, and there is 1% that said it's not important at all.

Next question is which safeguards could be considered? More than one answer is possible, multiple choice. I think maybe this will tell us that everything is important, and it kind of shows that way.

Waiting period for newly created accounts, that's 50...is that 2 or 3? I can't see, 52%, 53%. I need new glasses.

Requirements to hold domains through the add grace period without abuse action, 33%. I need new glasses. No unresolved abuse reports on initial transactions, that is 34%. Activity based trust scoring behavioral indicators, [inaudible] percent. Manual review before first API batch access, 38%? 36%, oh gosh, I'm so sorry. I should stop saying the percentage. And contractual reseller agreement requirements, 53%, right? 53%. And other is 11%. I can see 11%.

Third question, which approach seems more reliable for managing API access? This is a single choice. I'm going to go for the percentage there. That is activity-based friction, 21%. Identity-based verification, 10%. A mix of both, I think that's the most of us responding, 65%. Other, 4%.

And the last question here, if a registrar confirms a malicious registration is in an account, what could be considered to happen to that account's API access? Again, this is more than one answer possible. Immediate suspension, reinstatement after review, 45%. Temporary restriction pending investigation, 61%. Warning only unless repeated abuse occurs, 14%. No action, I'm so glad nobody picked no action. I was very scared when we put that in the poll that someone would actually click on that. And other is 5%.

So thank you for the responses. I think this is just taking the temperature of what the room feels and also to inform us on how we can properly scope and articulate the charter questions.

I'm going to throw to Feo.

FEODORA HAMZA:

We noted that we didn't show all the questions to the first topic or the results, so if it's possible to since we have a few more minutes on this topic and there are no other questions, maybe we could show them quickly as requested in the chat. So Question 2 and Question 3. Jen, I give it to you.

JENNIFER CHUNG:

I'm glad I can see this on my screen this time. So just backtracking through the discussion with the PDP structure, we didn't really go through the second and third questions. I think this was actually discussed, so I think it's important to take a look at.

So going straight to Question 2 it says for the PDP structure: If one topic should come first, which would you prioritize? This is a single choice only. For API access for high-volume registrations, 26%. Associated domain checks, 46%. Either/no preference, 28%. I think there is a little bit of a preference for associated domain checks to go first.

The third question is: What factors should weight most heavily in deciding the order of topics? Single choice. Ease of reaching consensus, 27%. Expected impact on reducing DNS abuse, 58%.

Resource and time constraints, 14%. Other, 1%. I think we have quite a lot of discussion on what the other is and also it does reflect on the choices here made on these two questions. So I think that's good. Back to Feodora.

FEODORA HAMZA:

Thank you, Jen. Thank you, everyone. Let us now turn to the second issue identified in the preliminary issue report called associated domain check. This was also identified as a priority gap in the DNS Abuse Small Team. It says that when a registrar confirms that a domain is being used for DNS abuse there is no contractual requirement to investigate whether the same registrant account or a related entity has other active domains engaged in similar abuse. In many cases DNS abuse occurs as part of a broader coordinated campaign that relies on dozens or even hundreds of related domains.

The absence of an obligation or requirement to examine associated domains can allow bad actors to continue operating their campaigns even after one abusive domain has been identified and acted on. Some registrars already perform such pivot investigation internally, however these practices are not applied uniformly. As a result some campaigns can persist longer than necessary as each domain is addressed individually and sequentially rather than at a portfolio level.

The NetBeacon White Paper and other community contributions have suggested introducing this associated domain check as a

requirement to help disrupt DNS abuse campaigns more effectively and reduce overall abuse, DNS [abuse uptime].

So similar to as discussed earlier...sorry. The objective of addressing this issue in the PDP would be to explore whether and how registrars should be required to conduct reasonable checks for other potentially abusive domains linked to the same account, registrar, or other relevant identifiers once one domain is confirmed to be related to DNS abuse or to be malicious.

The intention is not to impose on your burden or to overreach into customer portfolios but to establish a balanced proportionate obligation that improves responsiveness and consistency across registrars while maintaining fairness and due process.

So my question back to the community and the room: Did we get the scoping right? Are there any other charter questions you would like to propose that we should consider and also potential solutions. Just noting that many in the community provided potential solutions in their public comments, so this is also where the questions are based on and the answers. But we also are happy to hear more. Thank you. Jen?

JENNIFER CHUNG:

Thank you, Feo. I see a nice healthy queue building, but we will now launch the poll for this one. Again similarly, we're not trying to prejudge any outcomes of the PDP. This is to inform us whether or not we're scoping and articulating the charter questions correctly

and if there are questions we haven't considered. So please while you fill away this poll...I can't see my queue anymore. Sorry. Can we move that? Oh, okay. All right. Janos, please go ahead.

JANOS DRIENYOVSKI: Thank you very much. All these scoping questions are [irrelevant], I believe. The Public Safety Working Group would like to put emphasis on using systems for checks that already exist in terms of tracking. So we do not necessarily see a need to create new means of tracking but rather the contracted parties should use those means already available to them that they would already use for their customer management purposes. Thank you.

JENNIFER CHUNG: Thank you, Janos. Susan, please go ahead.

SUSAN CHALMERS: Thank you. Just a quick note that in the GAC submission the GAC had suggested prioritizing the associated domain check PDP because its scope and charter questions appear to be narrower than those involved in the other issues. So I just wanted to note that. Nothing to do with scope but just in terms of priority. Thank you.

JENNIFER CHUNG: Thank you, Susan. Well noted. Farzaneh?

FARZANEH BADIEI:

The questions that you have in the poll, as I mentioned, NCSG has concerns about associated domain checks and the questions here are very concerning. When we are thinking about them we just see how this thing can go wrong. I know that these are the questions that are preliminary, but I would appreciate if we can also think about all the implications for the users' rights, for the registrants' rights when we are thinking about these mechanisms like the timeframe or how do you verify it. One of the questions could be what do you think the human rights implication of this mechanism is?

JENNIFER CHUNG:

Thank you, Farzi. Well noted. We also note that NCSG did mention this in the preliminary report. I'm glad you also put this on record. A reminder for all of us, and I don't know if we are super familiar with our PDP process, but the human rights impact assessment is a mandatory segment in all of the PDPs that we'll be launching. So it's a good reminder if you don't already know this. And of course, we lean very heavily on the NCSG colleagues to give us a lot of expert advice and feedback on that, so we really appreciate that. Feodora, did you want to add? Okay, let's go to the queue. Owen, please go ahead.

OWEN SMIGELSKI:

Hello, Owen Smigelski. I'm with the registrar Namecheap. I'm chair of the Registrar Stakeholder Group, but I'm speaking as just a registrar in this capacity. I see on there the defining association account ID, registrant email, etc., for these associated domain checks. And I want to strongly caution about discussing these types of specifics publicly. Our goal here is to prevent bad actors from doing bad stuff, and we've found a number of times in the Registrar Stakeholder Group those of you may know that there's an abuse contact identifier tool, the ACIDTool.com, other registrars provide as a service to the community where you can look up registrant information, host information, email information. The two times that we've announced this publicly when it first came out as well as when we did significant upgrades it was immediately attacked within days by DDoS attacks and taken offline.

Well, at least the first time. Now we have a lot more horsepower of a server behind it to protect against these things and mitigate it. But we had something like 300,000 simultaneous requests within minutes after we announced the upgrades at Prague.

So the bad actors are paying attention to these things and if we discuss how do you define an association and put that into a policy, they have a roadmap on how to avoid that. And so while I think we should be encouraged to discuss these potential ideas, there needs to be flexibility and also a degree of confidentiality in what registrars can do. Because yes, those are four ideas up there, but there might be 20, 30, 50 things that registrars can look at. And if

we put all of those into a policy and discuss them, then we are defeating the purpose of having the associated domain checks.

So while I think it's good to talk about these in generalities, some sort of these specifics could actually harm an eventual policy that comes out when there's no need to do that and give them away to circumvent what we've discussed. Thank you.

JENNIFER CHUNG:

Thank you, Owen, for giving us the caution. And of course, registrar colleagues day in and day out do deal with this, and it's really important that we also take into account what happens when we're looking at this. Again stressing that this has been as open and transparent as possible, but we're not trying to give a blueprint for bad actors to be able to use these attack vectors to thwart our efforts.

Going back to the queue, Justine, please go ahead.

JUSTINE CHEW:

Thanks, Jen. I just wanted to note in addition to what you noted the fact that the future PDPs are going to have the human rights impact assessment check. In addition to that, it also would incorporate the global public interest framework checks as well. Thank you.

JENNIFER CHUNG:

Thank you, Justine. Very important also learning from the Latin diacritics PDP who I think was the first PDP to incorporate both of

these things into their discussion. So whatever PDP coming out of this process for DNS abuse has a lot to learn from that process too. I think it's Thomas. Thomas is next? Or, Owen, is that a legacy hand or coming back for more? Okay, Thomas, please go ahead.

[THOMAS]:

Yeah, I'd like to build on Owen's important comments that no company would publish it's IT security concepts, for example, or their contingency planning because that would open them up to being vulnerable. Maybe this is a good point in time to discuss this with this very group that in terms of expectations for the outcome I think we should allow for as much flexibility as possible for the contracted parties to find responses so that they are agnostic to specific solutions but just require them to efficiently tackle the issue in general. So I think for those who are expecting like if A, then you have to do B or something, it should allow for much more flexibility than that.

And I guess that will also allow for us to come to results faster if we don't try to be prescriptive because there are different business models. If you have a retail registrar, the solutions need to be completely different to if you have a corporate registrar, for example.

JENNIFER CHUNG:

Thanks, Thomas. Good reminder here as well. I see there is a queue but I also want to remind people in this room this is not just a

discussion with people who are sitting at the U-table. If you do want to put your hand up, please make sure you are in the Zoom room. We will follow the queue there. And there will be a mic either roaming around the room or you can come up to a free mic on the table to speak.

Let's continue with the queue. Margie, please go ahead.

MARGIE MILAM:

One of the things that we put in our comment was in addition to taking a look at these domains that are associated, to do a proactive contact verification at that point. And I think that typically your bad actors are going to be providing false information to the registrars. And if you do a proactive verification check at that time, you may end up having a faster mechanism of suspending the domain names. And that is consistent with the EU's approach and the NIS2 directive where the guidelines published by the cooperation group essentially said that. And I think this is one of those scenarios where it's probably a really good recommendation that would help speed up the process in dealing with these abusive domain names. Thank you.

JENNIFER CHUNG:

Thank you, Margie. Farzaneh?

FARZANEH BADIEI:

We have some concerns about requesting for confidentiality of all the practices. While we appreciate that there has some

confidentiality, it should not prevent accountability of whatever methods that you use. We need to have some kind of minimal transparency as much as possible while protecting the methods so that it cannot be abused.

One of the...we see it in other digital governance spheres that when companies get together and come up with a method that is not very transparent, for example hash matching, then there will be some potential impact on freedom of speech, human rights. And so we want accountability mechanisms in place while you can keep it confidential. But we have to discuss this a little bit further. Thanks.

JENNIFER CHUNG:

Thank you, Farzi. I think I recall in previous ICANN meetings there was very good cooperation of a joint session of the registrars and NCSG or NCUC did to go through some kind of scenarios. So I think a continuation of that or some form of that when we're looking at this might be very useful.

I think that is Marc Trachtenberg. Thanks.

MARC TRACHTENBERG:

I made this comment in the chat but I'll just make it here as well. I totally agree with Owen's point about how adaptive and sophisticated the bad actors are. They're constantly changing their methods. And I just can't help but wonder whether it makes sense to dedicate a massive amount of resources to two PDPs on two very narrow ways in which bad actors are engaging in DNS abuse. I

wonder if by the time we get to a solution it's not going to be relevant anymore.

I mean, with Agentic AI already bad actors are registering domain names in bulk not through API access. And similarly, we're already seeing that they've spread out their registrations across multiple registrars to avoid associated domain name checks by registrars that do that. And so does it make sense to dedicate all these resources to these PDPs, or is there some better way to address these problems?

JENNIFER CHUNG:

Thanks, Marc, for that. Just out of curiosity, do you have suggestions that we might consider as better ways to deal with this?

MARC TRACHTENBERG:

I mean, some self-regulation. Many registries and registrars are already working on some of these methods. But to have two PDPs that take a year for these two very narrow ways where bad actors are already going around them just doesn't seem like it makes that much sense.

JENNIFER CHUNG:

Thank you, Marc. We will consider looking at our charter and looking at the articulation of how we're trying to address the problem. Echo. Reg, please go ahead.

REG LEVY:

Thank you. Reg Levy from Tucows. I'm also co-chair of the Registrar Stakeholder Group DNS abuse subgroup and co co-chair of the contracted parties house DNS abuse subgroup. With regard to Farzaneh's point about making sure that there's recourse, registrars have an incentive to work with their customers, their good customers, to make sure that we aren't overcompensating for DNS abuse and to make sure that there is recourse.

So I fully understand your concerns in that regard but, and to Owen's point, I think that it should be up to each registrar specifically with regard to their business model and their customer type. Because as I think Thomas said, if you have a corporate registrar you are going to have different interactions with your customers than a standard direct-to-consumer registrar than a wholesale registrar. So there are many different business models.

And to Owen's point and to Marc's point, again each of us experiences a slightly different type of abuse and so each of us is going to be dealing with it in different ways and mitigating it in different ways. And so what we end up with is going to need to be broad enough to encompass all of the business models and also to not give the bad guys a map of how to do it better.

That said, I love Marc's recommendation that we just not do PDPs. This was however asked for by the community, and so that's why

we're here. But if you want to just let us do our thing, that's also fine.

JENNIFER CHUNG: Thanks, Reg. Now we have a queue that's growing. Next is Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Yeah, thank you. Chris Lewis-Evans from CleanDNS. Criminal behavior changing is a thing. I've seen it many times. So we do need to be very careful, to Owen's point. But I think we do need to be doing something.

We see a lot of people are already acting, and I think the point of this PDP is to make a good floor, raise that floor so more action is taken, less harm is caused. Best practice or contract changes, PDP recommendations need to be spread to everyone. And we can't do nothing because people are already acting. But things more need to be done.

So that needs to be contained and shared, but it might have to be a bit more nuanced so we don't reveal techniques. But something does need to be done for everyone, not just the people that already carry it out. Thank you.

JENNIFER CHUNG: Thank you, Chris. Good reminder as well. Next we have Nick.

NICK WENBAN-SMITH:

Yes, thanks. Just in terms of this specific question, I think the most obvious use case that I tend to see in my day-to-day job as general counsel for a big ccTLD is you have a report of malicious activity, bad acting and you look at the registration records and it's clear and it becomes fact. This is obviously a fake ID. And then I don't see why it's so complicated that if you've got a proven abuse report with proven fake ID, that that's just not a complete blanket shutdown for all of the other registrations with that exact same registration information. That's the most primary use case you can have. I don't understand why it's so complicated.

And the second thing, and I think this is the point maybe to try to get into the PDP framing, is that obviously that same fake ID is not just used with one registrar on one account. It's also used in multiple accounts. And so it would be very beneficial if some better coordination of those known proven fake IDs could be better shared and socialized across the different registrar accounts so that you could address the same issue across multiples.

Because we see frequently that say there's a campaign to register fake further education institutions which is common in terms of abuse, it's not just one registrar which has used it but you can see the pattern across the different registrars that the same strings and patterns are registered in quite close proximity across multiple different registrars in order to evade the detection systems. So that is just something that it would be nice we could socialize that

actually to get better solutions across the community through these sort of PDP processes. Thank you.

JENNIFER CHUNG:

Thanks, Nick. I'm going to do a little bit of a prerogative by being the facilitator and kind of push Reg up on the queue. I think she has a direct response. So if that's okay with Janos and Thomas, we will have a little bit from Reg as a response first. Can I see some smiles so I think it's a yes? Please go ahead, Reg.

REG LEVY:

Thank you. Often we don't see fake information to the extent of Mickey Mouse at 123 Main Street. We see stolen information. So Reg Levy is using Nick's information. And I hope that you're not suggesting that we further the harm to the person whose information has been stolen by me sending to my colleague Namecheap that Nick Wenban-Smith is out there being used by everybody. Here's all his information, his phone number, and everything.

There is communication within the community. There are certain bad actors that we know, and we do share their information with each other. Because as they change we say, hey, this guy is performing an attack on us. You guys might see it soon too. But those are unique and rare. And I want to be careful about mandating that we share information about our customers with

our competitors because that also seems like a weird path to go down.

I understand where you're coming from and we do want to resolve DNS abuse. We want to be helpful. We want to have these conversations. But we do want to be careful about how we're recommending that happens.

JENNIFER CHUNG:

Thanks, Reg, for that reaction and the reminder as well to think about it in the registrant context as well. Now we go to Janos.

JANOS DRIENYOVSKI:

Thank you very much. That's a lot of valuable discussion and very important questions as well how we will approach this. And any policy regulation when it comes to Internet governance or any digital technology related areas is always difficult because of emerging technologies development. So I would just react on that point that it perhaps would be helpful to include a question for both topics to ensure that solutions are future proofed in relation to emerging technologies would be perhaps something to consider. In any case, this should be also in the forefront of our minds to whatever we produce in a PDP, in a policy, or whatever it is, obviously it will be future proof and will stand the test of time. So it's just a suggestion.

JENNIFER CHUNG:

Thank you, Janos. Very important suggestion. We should be that way and have the balance between prescription of certain things and actually also looking forward to a future forward kind of solution as well. Thomas?

[THOMAS]:

Yeah, thank you so much. For those who have monitored the queue, they may have noticed that I put up my hand and then I took it down and then I put it back up because I may be stating the obvious. But Marc's intervention made me think that certainly in an ideal world everybody would be doing the right thing and there wouldn't be any need for action by this group.

Let's not forget, this is self-regulation, right? If we are doing policy, that is self-regulation. But it needs to work. And while it's not directly applicable if we look at the way the contract amendments that the contracted parties made, they had an effect on bad actors. I think that shows clearly that if we tweak a little bit here and there, we don't ask too much of the good actors but we give ICANN a tool to investigate and terminate the contract and escalate with the bad actors which are unfortunately also in this ecosystem.

JENNIFER CHUNG:

Thanks, Thomas. Reg, legacy hand or back in the queue?

REG LEVY:

Legacy hand.

JENNIFER CHUNG: You don't want to take another shot?

UNIDENTIFIED MALE: Give her another shot.

JENNIFER CHUNG: Okay, Rod Rasmussen?

ROD RASMUSSEN: Hi, I'm here observing for the SSAC as well just speaking again as a professional in this space. One thing that we've been doing here is kind of assuming that there is a bad actor that is creating an account and registering things. Another avenue though is for bad actors to take over somebody else's account, right? And that has two implications, I think, that are important for the work to consider.

One is you should be doing an associated domain check because you may have a compromised customer, not just because there might be a bad actor. So this should be kind of baseline, I think, anyway. And I think most registrars who know what they're doing are doing that because you don't want your customer to be abused.

Then the other part of that is separating out the good from the bad within that account. So in other words, you may have a long-term customer that has registered a few domains and then all of a sudden there are 10,000 new domains that are launching phishing

attacks. Access to that account may need to be temporarily suspended while you figure that out, but these are the kinds of things that you have to consider as you're going through this and not just assume that there are just bad actors and good actors and that there's no intermixing.

So I just wanted to point that out as part of the chartering questions and things like that to take that into account. Thanks.

JENNIFER CHUNG:

Thanks so much, Rod. This is exactly the feedback we want and discussion we want from the community because we really need to articulate these charter questions correctly if we're trying to get to an efficient process when we're looking through the PDP. And of course with the right questions, and I heard from our NCUC colleagues that we need to ask the right questions as well.

Oh, we have more of a queue. I thought we were going to wrap. Sourena, please go ahead.

SOURENA MAROOFI:

Hi. Rod already mentioned one case that may happen that the domain is compromised. There are other cases like that. For example, I put a public comment actually mentioning and also [inaudible] public comments [inaudible] shows that, for example, there is [a lame] delegation. There is domain with a [dead] name server that they're compromised. And unfortunately, the registrar takes down all other domain names of the same registrant.

So I believe that it's not like all the registrars they know what they are doing. I know that they are expecting their [inaudible], but there are cases that actually they've taken down all the domain names of the one registrant that are not necessarily malicious. Thank you.

JENNIFER CHUNG:

Thank you, Sourena, for that comment. I don't know if there's any response to that or any necessary response to that. If not, let's take a look at the results of the poll. I hope it shows up on my screen so I don't have to squint and do another eye exam.

Okay, associated domain checks: Should registrars be required to investigate other domains associated with a customer when one is confirmed as malicious? 52% say yes always. 33% say yes in specific cases, for example repeat abuse or verified evidence. 12% say no it should remain voluntary. 2% say other. I'm always really curious about the people who say other. I hope they already spoke up. If not, please put your hand up.

Second question: Which criteria could be valid association points in this regard? More than one answer is possible. Multiple choice, I love multiple choice. 74% say same customer account ID. 75% say same registrant email address. 76% say same payment instrument or billing information. 54% say same IP address or hosting environment. And there's a whopping 19% that say other. Please, if you haven't told us what the is, let us know.

Third question: What, if at all, would be a reasonable timeframe for completing associated domain checks? Single choice. 32% say within 24 hours. 23% say within three business days. 8% say within a week. 31% say case dependent or flexible, and 7% say other. This has a lot of timing there.

Okay, fourth question says: What documentation of an investigation could be considered to demonstrate accountability and compliance? Single choice for this one as well. 43% say summary level notes, for example checks performed and outcome. 26% say detailed logs that include timestamps, review steps, decisions. 21% say only retained if enforcement action taken. 4% say no formal documentation required, and 6% say other.

Okay, that is interesting. I think that kind of reflects what we were discussing so far. I do see a hand up. Reg?

REG LEVY:

Sorry, can it be put back on my screen? Sorry, I'm speaking as one of the other and now it's time for me to have an eye exam. Thank you very much. Okay, so with regard to the requirement to investigate other domains when one is confirmed as malicious I put other partly because of the conversation that we were having earlier. So there is a difference between a new account with four domains and one is definitely malicious and an old account with four domains and one is definitely malicious.

So I just wanted to encompass the fact that there are many different situations, and so that was the point of my other. That this feels very prescriptive and I think that we need a better and more flexible approach than many of these questions reference.

With regard to criteria, I do understand that multiple things are available. But I did answer other specifically and not just these because we have a lot of data points and we have different data points. Roger is over here nodding at me with many of the things that I say, but we have very different data points between our two companies. And probably he has different ones even than the other two of us.

So some of these are things that I might consider, but also I have other things that I might consider. And also, also, there are not going to be one answer. So it's not necessarily going to be just the registrant email address that's all I'm looking at and if it's the same, then blitz the account. We're going to have to take a holistic look at this.

Which brings me to my answer to the third question which was also other because since it is a holistic look at the account, someone is going to have take some time. Sorry, not the third answer. The fourth answer. Someone is going to have to take time to look at this account and make a determination, and that's not necessarily going to be documentable.

This says log files. I don't know that that means. Does that mean that one of my team members logs into the reseller account to look

at the registrant information in all other domains in that reseller account? Maybe it does. We might log part of that. Like we can log that my people log into the reseller's account because that's obviously a loggable. But just looking at the domains, that's not something that we keep logs on. So are you asking me to create logs of things that don't exist now? Please don't do that to my tech team. And we can also perform a search for just the email address within our system across resellers, and that's also not something that we log.

So I don't know. Currently, there are a lot of things that ICANN Compliance audits us on, and they can take our word for some things. And I don't know that every single one of these is necessarily going to lend itself toward filling out some sort of a document that says I swear on this date I reviewed domains associated with this bad domain, sign here, and then we file it away in case anybody asks us about it.

So I'm a little concerned around the implications there. I like to always say that I'm the edge case, so if other is an option I'll typically take it.

JENNIFER CHUNG:

Thanks, Reg. I think it's a good reminder for us to also think about it in a holistic way. I think this is not to prejudge any kind of determination by the PDP process that will come up but to spark some conversation so we can articulate the charter questions in a

way that allows us or allows the PDP working group to be able to think about it in this way.

I've lost my queue. I have my queue. Farzaneh?

FARZANEH BADIEI:

I just wanted to reiterate what Bruna said in chat that if we have...maybe the PDP can touch upon accountability recommendations so that it can also remediate our concern about practices that have to be kept confidential but it could potentially have impact on the registrant's rights. Thank you.

JENNIFER CHUNG:

Thank you, Farzi. And I think we have Margie with a final word before we wrap. Margie, please go ahead.

MARGIE MILAM:

Thank you. When I checked other I was thinking about my earlier comment where you're talking about association and you're looking at more than just the account ID. I think this is similar to what Reg was saying. It's really the registrant's contact information to see if there's any association with the actual registrant. And that's something that doesn't seem to be suggested here, but I think it's something that is important to be included in part of the discussion for the PDP. Thank you.

JENNIFER CHUNG:

Thank you, Margie, for that. And I love being very punctual with this session. I think this session has been really helpful for all of the community to actually surface some good questions, good discussions. All of this input will be taken into account when we look into refining the charter questions looking at the final report. Again, this DNS abuse mitigation topic is extremely important to all of the ICANN community and also outside of the ICANN community as well. So we really appreciate all the engagement. And those who are in the room as well, thank you for filling out this room. I think it's very evident that people find this very important.

The next steps, if I've missed any, staff, please chime in. I'm looking at the shakes. The next steps are going to be the final report. Council will then look at it and hopefully we'll get the PDPs started as the community is expecting with a good timeline, with efficient timeline but answering the right questions in the right way, holistic way. I think I've hit on all those key terms. I think someone was doing a bingo. I'm not sure if...tell me what I have to say before I stop saying things.

But thank you very much for your good engagement and looking forward to continuing this discussion. Thank you very much.

[END OF TRANSCRIPTION]