JULIE BISLAND: All right, for the recording, this is Julie Bisland. Good morning, good afternoon, good evening, everyone. Welcome to the DNS Abuse Mitigation PDP-1 Working Group call, taking place on Monday, the 30th of March, 2026. For today's call, we have apologies from Mary Penn, IPC, and Matthew Thomas from SSAC. I think Eberhard Lisse has joined. We have alternates joining today, David Hughes from the IPC.

Statements of interest must be kept up to date. Does anyone have any updates to share? If so, please raise your hand or speak up now. All right, seeing no hands. If you need assistance updating your SOI, please email the GNSO Secretariat. All members, participants, and alternates will be promoted to panelists. Observers will remain as an attendee and will have access to view chat only.

All documentation and information can be found on the DNS Abuse PDP-1 Working Group wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name before speaking for the recording. As a reminder, participation in ICANN, including this session, is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct. Thank you. And now over to our chair, Paul McGrady. Please begin, Paul.

PAUL MCGRADY: Good morning, Julie. Thank you. Good morning, afternoon, or evening, everyone. Thank you for joining. This is item number one, welcome.

Item number two, we have a Chair and Vice Chair selection done. I want to congratulate Nick Wenban-Smith as our Vice Chair winner.

Staff will post the actual stats here in a little bit, but we had a clear winner. Nick, thank you for your spirit of volunteerism. We are going to get you onboarded. Welcome to the fun. Nick, do you want to say something? Say hello and welcome.

NICK WENBAN-SMITH: I am a bit surprised and very honored, actually. I am very touched, so thank you for your support and trust. I will try to make sure I repay that. Thank you.

PAUL MCGRADY: Thank you, Nick. I appreciate that. All right. Next up is meeting cadence. We had the initial question about Easter Monday, which led to a discussion about how many meetings are actually on Monday all around the world, which of course we are a working group that is all around the world.

It turns out that there are a significant number of Mondays that would be disrupted if we pushed our Monday meeting or canceled our Monday meeting, whatever we decided to do. I think that the conclusion here, with this many disrupted meeting days, is that Monday is not the best day for us. So, we took a look at the second-best day and time, which is relatively around the same time or maybe even the same time as this call, but on Tuesdays.

Tuesdays, after research, have far fewer public holidays, approaching zero. We are taking a good look at moving the meeting to Tuesday. We are going to take a queue on that, and then leadership will take it back for discussion. Reg, I see your hand is up. Go ahead.

REG LEVY: Hi, thanks. I note that Mondays are frequently holidays observed, but we have already scheduled it, and holidays change around the world, so I would advocate for not moving it, even though I would get an extra hour of sleep. However, if we do move to Tuesdays, then we really need to look at the ICANN events. Not so much the holidays, but the actual events that ICANN puts on. The Contracted Party Summit and the actual ICANN meetings should be taken into account.

PAUL MCGRADY: Thank you, Reg. Absolutely. On the summit and the actual ICANN meetings, we will be...

JULIE BISLAND: Hey, Paul, your audio went very quiet.

PAUL MCGRADY: Is this any better?

JULIE BISLAND: Nope.

PAUL MCGRADY: Great. I guess I will talk as loud as I can and hope that works.

JULIE BISLAND: I do not think it is going to work. Why don't you dial out to my mobile number?

TERRI AGNEW: It sounds like another speaker picked up versus your computer speaker. Do you have AirPods nearby or something?

PAUL MCGRADY: I do not, no.

JULIE BISLAND: That is better, Paul.

PAUL MCGRADY: This is better?

JULIE BISLAND: Yes. Whatever you did worked. Do not change anything.

PAUL MCGRADY: I did not do anything. Yay, technology! I am not sure where we were. I was responding to Reg. Yes on the Contracted Parties House Summit.

When it comes to the actual meetings themselves, we are going to have significant meeting time together in Spain. That will be taken into account. Brian, go ahead.

BRIAN CIMBOLIC: Thanks, Paul. I do not know if anyone else found themselves in the same boat, but I know when we announced the Monday meetings, I removed a series of internal meetings to be able to make these. I would love it if, to the extent we identify the Mondays that are really problematic, we just move the meetings to Tuesdays for those identified weeks.

I know that becomes a little hard to just assume you have the Monday morning meeting, as it involves checking the calendar, but that may be easier for myself and maybe other people rather than reshuffling other internal meetings and schedules. It is just something to think about.

PAUL MCGRADY: All right. Thank you, Brian. So we have two advocating for not changing Monday. I presume, Reg, by not changing Monday, you do not mean cancel, you mean push them to Tuesdays?

REG LEVY: Correct. I do not think that we should cancel because of holidays because we would just be chasing holidays. We would do without some people, and we would be poorer for their lack. However, either we switch those specific ones to a Tuesday, or we just have the events.

PAUL MCGRADY: Gotcha. Okay. Thanks, Reg. Any other comments on this? I see some folks in chat, but it is hard to read chat and watch the other queue. If you feel strongly about this, please step up and turn on the microphone. Gabe, please go ahead, and then Nitin.

GABRIEL ANDREWS: Hi. This is going to be very selfish for those who are on Pacific Time. When we attend at this time, it is essentially 05:30 AM on a Monday. I note that there is some difficulty for those whose brains are as slow as mine to recall the discussions that occurred the prior week. If it was switched to a Tuesday, that is one day more just to get back in the swing of things. I would put a plus one for that reason, if for nothing else. Over.

PAUL MCGRADY: Okay. Thank you. Nitin?

NITIN WALIA: Thanks, Paul. I would like to second the view of keeping it on Monday because we have already aligned our schedules keeping in consideration that this meeting was going to be held on Monday. I believe it would be beneficial if we keep this on Monday at least until ICANN 86, and then if we need to replan our calendars, we can have another poll and decide accordingly. Thank you.

PAUL MCGRADY: Anil? Are you there?

ANIL KUMAR JAIN: Thank you, Paul. Anil for the record. First of all, I would like to congratulate Nick for the Vice Chair position. I hope that now the leadership position is complete, we should move very fast. Second, about the selection of Monday or Tuesday.

Initially, if you remember when we were discussing the dates and days, I said any day is okay with me and we can go ahead with any day. But I respect the view of most of us that we should not change. In case there is any holiday, a holiday may happen with some of us at any time, maybe on Tuesday also. Sometimes we have to miss and go to the wiki page to cover up whatever was lost. I also support that we should continue to have it on Monday. Thank you.

JULIE BISLAND: Paul, your audio went down again. Now we can't hear you at all. Better. Good.

PAUL MCGRADY: Is it better all of a sudden? Julie, maybe what we do is have staff do the update on the work plan while I go on mute and you can dial out to me so we can fix this over the phone. Anyway, I was just thinking about the last comment on the public holiday thing. If holidays can happen at any time on Tuesdays and we will be chasing holidays, what do we do with those Tuesdays that we reschedule? We need a stable schedule in order to get the work done.

All right, I will take all that back. Nick and I will talk to staff and reach a decision about what to do about Easter Monday and follow on all the other Monday holidays we find ourselves in. For the next PDP Phase 2, whoever is going to be chairing that, Mondays should be off the Doodle. All right. Let's go ahead with the next thing, which is an update on the work plan. I am hoping that John can jump in and start that while I go on mute.

JOHN EMERY: All right. Thank you so much, Paul. We will go ahead and get back to everyone on the meeting cadence. As noted in the chat, based on the Doodle poll, Monday was the number one time and the proposed Tuesday time was number two. Leadership and staff will take you through that.

Update on the draft work plan. This was the initial timeline and milestones, just as a reminder. I have dropped the draft work plan spreadsheet in the chat, which all of you had a chance to comment on. Based on taking everything into consideration and feedback from the working group and at ICANN 85, leadership and staff were able to update the timeline a little bit.

Basically, we updated the deliberations based on the April start in general. The real difference here is the compression. We were able to find dates and times in the schedule to push up the date from October or November 2027 to May or June 2027. If Paul wants to chat it through or if he is getting the audio together, we can start a queue. Based on feedback, this is where the updated timelines and milestones ended up

based on the required times for ICANN bylaws for public comment and proposed times based on diligent asynchronous work.

TERRI AGNEW: All right, Paul, you are going to have to press star six first to unmute your phone. Sorry. There.

PAUL MCGRADY: Okay. That is all right. We just patiently will defeat the technology. You just have to keep pushing through. Can everybody hear me now?

TERRI AGNEW: Yes, Paul, we can.

PAUL MCGRADY: All right. I am getting a John. Okay, there we go. This is the timeline that John just walked us through. I see the chat is very active and still about the holiday issue. We will let that sit, but I will do my best to keep an eye on the chat regarding the actual work plan.

This depends on a couple of things that we talked about at our face-to-face meeting. This is an aggressive timeline. We have cut as much fat out of it as we can practically under the bylaws. The only thing that we can do to accelerate this is to get our work done sooner. That relies on us. We had a request early to go from four hours of meetings a week to an hour and a half. We want to honor that, but the trade-off there was no pontification and no repetition to drive the point home. I think

actually, so far, we have been doing pretty well with that. Let's keep that up. Any questions about this timeline? I will open a queue. At the end of this call, if this is stable, it is going to Council through Jen. Seeing no hands. Farzi, please go ahead.

FARZANEH BADIEI: Hi. Bruna keeps saying in chat that she cannot raise her hand. I just wanted to know if she has a point to make on this one. My question is, initially we had October until November 2027, which would be a year and a half. Now it is going to take us one year to finish this work, right?

PAUL MCGRADY: That is right. If you streamline this and you presuppose an aggressive number of working sessions in Seville, we think we can get it done. Staff is currently working on getting us at least four hours together, maybe a bit more.

FARZANEH BADIEI: Okay. I am not confirming or objecting. I am just verifying. Thank you.

PAUL MCGRADY: Thank you. Martina, go ahead.

MARTINA BARBERO: Thank you very much, Paul. This is Martina from the European Commission, representing the GAC for the record. I just wanted to thank you for reviewing the timeline because this was a message coming from

the GAC during the last ICANN meetings that we wanted to see something slightly shortened. This is really appreciated.

The question from our side was linked to the fact that since this is such a targeted and narrowly scoped PDP, and since what we were presented last time was the average time that it takes to go through the deliberation and all the steps, it is nice that this tailored and narrowly scoped aspect is reflected in the timeline.

I was working on a previous timeline and expecting to provide comments on how we could shorten and be more effective on the deliberation. I understand that now we have until the 3rd of April to comment on the new timeline. Let us bring that back to the GAC and see if there is any further comment or concern. Thank you.

PAUL MCGRADY: Thank you, Martina. Yes, we have until April 3rd. In those comments on the timeline, if people have ideas about how we can make this even more efficient to speed things along and keep us on track, we are very happy to have those in the draft work plan. Anil, go ahead.

ANIL KUMAR JAIN: Thank you, Paul. Anil for the record. First of all, I would like to thank you and the staff because, as an ISP, we submitted a modification in the work plan which was a reduction of two months in submitting the initial report and a two-month reduction in getting the public comment. I am really thankful that it is considered good and accepted. We will try to

see in case we can suggest some more modifications to make the whole PDP more efficient until the 3rd of April. Thank you.

PAUL MCGRADY: Thank you, Anil. I see Volker's comment: "I'd like to spend more time talking about substance rather than timelines." I would too, but unfortunately, when you kick off the PDP, you have to sort of set the table. I hope we are coming up on the end of the setting-the-table exercises. We have to deal with holidays and timelines and all that good stuff, but let's see if we can knock this stuff out and focus our time on work. Ching, go ahead.

CHING CHIAO: Thank you, Paul. This is Ching from the BC. A quick question on the timeline. I understand that it is open for comments, but is the newly adjusted timeline based on a rough estimate, or is it based on the observation from those early inputs that we will be able to cut short? I would just like to get a sense of that. Thank you.

PAUL MCGRADY: The timeline was not cut based on early substantive inputs. It was based upon listening to the community in Mumbai, taking a look at how we are working already as a team, and examining the timeline to see what was put in there to be cautious rather than what was mandatorily required under the bylaws.

On top of that, we have the commitment from staff to give us a good amount of meeting time in Seville. This is where we landed. We did not

reduce the timeline because we are going to accomplish less work. We reduced the timeline because nearly everyone in the community would like to get this done as quickly as practical. This is a very tightly scoped PDP. It does not need to go on for years and years.

I do see in the chat from Farzi, Bruna, and others that they are concerned this is a significant cut and do not want us to talk about cutting it even shorter. I will echo that the need for speed has to be balanced by a need for quality. We are proposing this reduction but relying on everybody to do good work and stay focused so we have good quality output. I think that is the end of our queue. April 3rd is the deadline for comments, so please go ahead and add those in. We will get this finalized and then on to Council. We have an April 7th deadline to do that. All right. Let's move on to Volker's favorite thing: substantive discussions.

JULIE BISLAND: Yes.

PAUL MCGRADY: We received some early input from the BC, the GAC, the IPC, the ISPCP, the NCSG, and the registrars. We have a link in the chat on the wiki which includes the community input on the wiki and the inputs in a Google Doc. John, did you have something you wanted to say about these?

JOHN EMERY: Yes, just real quick. The community input on the wiki is for everyone to see. Those are just the PDFs. Staff put it together in a Google Doc with a hyperlink to each individual one broken down into tabs so you can look between them easier. As we go forward, we will be putting it in our collaboration document based on each charter question. We will be synthesizing it there. I just wanted to highlight that.

PAUL MCGRADY: Perfect. As John mentioned, the collaboration tool will be updated with these inputs so when you see questions one through four, you will see the early inputs there. These are being used as a pump-primer to get the conversation going and ensure we do not forget to consider them. We thought that was a better use of these than treating them like a public comment and spending weeks going over each one. It is a good way to see what other people are thinking early on.

We are back to charter question number one: what triggers the requirement to investigate associated domain names? Overarching themes based on discussions so far. Theme one: establish a trigger for the associated domains check. Obligations for registrars to conduct an ADC should be triggered only when the registrar has actionable evidence that a registered name is engaged in DNS abuse as defined in the RAA. The charter notes that the trigger should be tied to confirmed abuse where at least one domain is found to be engaged in DNS abuse.

Theme 2A: clarify the proactive nature of the contractual requirement. Once the evidentiary trigger is met, registrars should be able to proactively investigate associated domains linked to the reported and

confirmed malicious domain rather than waiting for additional reports. The charter states the policy aims to create a proactive obligation to investigate associated domains once abuse is confirmed. This supports more effective disruption of abuse patterns while remaining bounded by the evidence-based trigger.

Theme 2B: applying the ADC on a risk-based approach. Registrars should be required to conduct ADC only where there is a reasonable basis to believe associated domains may exist based on information available at the time. Members noted concerns that requiring ADC in all cases would create unnecessary burden and detract from addressing actual DNS abuse. Suggestions for reasonable indicators include multiple reported domain names, naming patterns, repeated reports, or customer risk profiles, supporting a flexible, intelligence-driven approach.

Theme 2C: define ADC as a two-step obligation. The ADC obligation could consist of taking reasonable steps to identify associated domains and then investigating those domains to determine whether they are engaged in DNS abuse using information reasonably available. This involves a structured process of identification followed by investigation.

Early input from the BC boiled down to: "A registrar shall initiate an associated domain name check when it is determined based on actionable evidence that a domain name under its sponsorship is engaged in DNS abuse as defined in the RAA." Input from the GAC suggests the requirement should be triggered when the registrar has actionable evidence that a registered name has been used, is being used, or is likely to be used for DNS abuse.

The IPC input says receipt of actionable evidence of DNS abuse from anyone, whether it be law enforcement, intellectual property rights holders, cybersecurity professionals, child safety organizations, or consumers, could prompt an investigation to identify associated domain names sponsored by the registrar or its affiliates. The ISPCP recommends the trigger be set at a meaningful evidentiary threshold, not merely the receipt of any abuse report. They caution against triggers based solely on third-party abuse reports, which vary widely in quality and reliability.

They suggest a determination following investigation that the domain was registered for malicious purposes, not merely suspected. The determination must relate specifically to RAA DNS abuse categories: malware, botnets, phishing, pharming, or spam as a delivery vector. The registrar should have a reasonable basis to believe associated domains may be part of the same campaign rather than being required to pivot automatically based solely on account linkage.

NCSG input: any obligation for a registrar to review domains reasonably associated with a domain subject to abuse mitigation can be triggered only when there is credible and substantiated evidence of DNS abuse consistent with Section 3.18 of the RAA. There must be clear indicators that other domains registered maliciously by the same customer may be involved in the same abusive activity using information reasonably already available.

The RrSG input: following mitigation of DNS abuse as described under RAA 3.18, and where reasonable evidence of systematic abuse or a consistent pattern exists, the registrar may conduct an associated

domain check. We have some variation here. Let's see if we can make the collaboration doc a little bigger. We have a good amount of time left. Let's jump in and see if we can synthesize the themes and inputs. Volker, I saw your hand up.

VOLKER GREIMANN: Thank you very much. Regarding the various straw men we have seen, I have a question for members of the RrSG. As Robert A. Heinlein wrote in his 1966 classic, The Moon Is a Harsh Mistress, "there ain't no such thing as a free lunch." Everything we propose comes at a cost.

Those who proposed that the trigger is just having one confirmed abuse report mean that the entire process of doing the checks for other domains will trigger on that. A lot of resources will be wasted that could be actioned for other abuse complaints. Is everyone who makes that suggestion aware of those costs? It will lead to slower abuse handling overall, and I fear that might not be the ultimate goal of all participants. We might want a more structured trigger. Thank you.

PAUL MCGRADY: Thanks, Volker. Marc, your hand is up. Go ahead.

MARC TRACHTENBERG: I think the trigger has to be when there is actionable evidence of DNS abuse for a domain name. It is true what Volker says that this may slow down some processing, but to not have that be the trigger vitiates the entire point of this PDP, which is the requirement to check for associated domains. I do not know what the standards will be for how

someone might think they have actionable evidence but not know to check without checking for associated domains. To not have that be the trigger does not make sense and makes this whole PDP pointless.

PAUL MCGRADY: Thanks, Marc. I guess, Volker, maybe you can respond to that. From the outside, somebody reporting abuse cannot see the patterns that would make it an efficient investigation in the sense of some of the triggers you are thinking of. How do we bridge that gap between what you are saying and what Marc is saying?

VOLKER GREIMANN: I think the gap is not quite as big as you perceive. Marc is absolutely correct that having actual evidence of abuse is part of the trigger. It is a very important part and probably even the major part. The only question is, does there have to be anything more than that? I think it would be helpful and beneficial to the entire community if there is. I feel we should be appreciative of the work that the contracted parties are already doing and try not to be wasteful to make sure we are more efficient in actioning abuse. The faster we can take down abuse, the better it is for everyone.

MARC TRACHTENBERG: I absolutely appreciate what Volker is saying. I just do not think that it reduces efficiency. I think it increases efficiency. That is the whole point. Yes, there are situations where you do a quick check and no other associated domains are found. There may be one-offs. But in many

cases, based on empirical evidence, bad actors register multiple domain names. It could be across registrars, which is a different problem, but we see bad actors registering multiple domain names at the same registrar.

That is where you get the efficiency. Where you see the one bad domain name, the obligation is to check for other related domain names so they can all be taken down at the same time. Are there efficiency costs? Yes, probably, but this is the point of the PDP. We identify these other ones, take down the entire cloud in the registrar, be done with it, and move on.

PAUL MCGRADY: Thanks, Marc. Farzi, I was going to see if I could get you to hop on because I saw your comment in the chat. You said one bad domain is not a threshold. I was curious about that. How many bad domain names does it take? Or is it one bad domain name that is super bad? We have to move from this idea, found in the registrar early inputs, which use the word "may." We see the registrars want a more permissive approach. Others say one bad domain name should trigger it. Where do we set the knob? What are the factors? Go ahead.

FARZANEH BADIEI: Great. Thank you, Paul. First of all, what do we mean by "bad domain"? This is very ambiguous. Are we saying a domain that is actively engaged with abusive activity as defined by the contract? What is our definition of "bad"? I really discourage using terms like bad and good because it is just ambiguous.

We have said time and again that we need qualitative indicators as well as quantitative indicators. When you say one domain is bad, you are relying on a number without defining what bad is, which is necessary for considering the threshold. This number might change under different circumstances. If there is a heavy botnet attack and one domain is engaging with botnets, then yes, that one domain could be a threshold. In other circumstances, it might be different. We need to discuss these things more and be a little bit less absolute. Thank you.

PAUL MCGRADY: Thanks, Farzi. I took the word bad from your comment, actually. One bad domain is not a threshold. We can back off using the word bad, but it is a good exercise accidentally. We have different suggestions on what that would mean. Brian Cimbolic suggests it means a malicious registration under 3.18.2. Marc Trachtenberg suggests it means a domain name involved in actual evidence of DNS abuse. I do not know if those are the same or variations, but let's hear from everybody. Gabe, go ahead.

GABRIEL ANDREWS: Hi, this is Gabriel Andrews for the record. A comment from the GAC's initial input under question two is relevant here. When we talk about associated domains, I think it is constructive to consider how they are associated. The GAC is suggesting that associated domains are those being used by the same threat actors and/or used in the same abusive scheme. We are not talking about all domains you might otherwise associate, but only those linked in those two categories.

Speaking in my own personal capacity as someone who has done investigations, Volker, in response to you, I would suggest it is constructive. Even if there is a report of a single domain where there is actionable evidence of abuse and malicious registration, I have seen occasions in which a bad actor will have a homoglyph domain, a lookalike domain, impersonating the victim, and it will be one of two dozen victims.

If a credible, actionable report of abuse from one victim with a homoglyph domain is made, it would make sense for a registrar to look under that portfolio of the customer account and see if there are two dozen other domains that are all obvious homoglyphs. I can take action against all of them simultaneously based off this one initial abuse report. There is an extreme benefit to this policy where you can take that amount of scalable mitigative action. I think that is the ideal we are shooting for. Hopefully, that is a constructive comment that is well taken. Go on.

PAUL MCGRADY: Thanks, Gabriel. All right, we have Marc, then Brian, and then Volker.

MARC TRACHTENBERG: Brian and I agree in the chat that we are saying the same thing, but I think the trigger has to be at least one domain. When you have actionable evidence that a domain name is being used for DNS abuse, the definition of which is narrow and describes bad activity, it is likely that if the same registrant has other domain names registered with the

registrar or under common control, those are probably being used for DNS abuse as well. Maybe not, but probably.

I think the trigger has to be that single domain name that indicates actionable evidence of abuse. The purpose is to be efficient and catch as much abuse as possible. The only logical way to do it is not just to look for other domain names being used for similar DNS abuse purposes. That is not efficient. The most efficient way is to use metadata factors to find other domain names likely under common control, in the same account, or using the same registration information. You identify all those, look at them, and see which ones seem to be used for DNS abuse. That seems logical, most efficient, and aligned with the purposes of this PDP.

PAUL MCGRADY: Thanks, Marc. Just to refocus us, we are talking about the trigger that kicks off the process as opposed to what we do once the process is kicked off. For those who do not want it to be based on one single report founded with actionable evidence of malicious behavior, what is that trigger then? What makes you look in the first place? That is the trigger, not the follow-on consequences. Brian, go ahead.

BRIAN CIMBOLIC: Thanks, Paul. Taking a step back, let's look at a typical fact pattern. We are talking about a registrant found to have registered a domain for purposes of carrying out DNS abuse. If I register gov-irs-login-secure.tld and it is found obviously to be engaged in phishing, I think it is fair to

have that as evidence enough to look at other domains in my account. That is very clearly set up for the purpose of phishing.

I am going to point to the language of 3.18.2. The current standard for when a registrar needs to take action on DNS abuse is when it has actionable evidence that the registered name is being used for DNS abuse. That is the existing trigger on a one-off basis. Volker mentioned there might be times where a one-off domain is enough to trigger an associated domain check. He is right after me in the queue, so I would ask him to tease that out.

I do not want to create a policy that becomes unenforceable. There are registrars out there with small volumes of new registrations but enormous volumes of malicious registrations. They have an outsized footprint of DNS abuse, typically linked to campaigns. I do not want to put ICANN compliance in a position where those registrars can shrug their shoulders and say they are only dealing with DNS abuse on a one-off basis because they did not have indicators of a campaign. We have to have this be enforceable. The point is to disrupt DNS abuse campaigns at scale. If we do not tie the trigger for associated domain checks to a one-off case, I do not think we have necessarily fixed anything.

PAUL MCGRADY: Thank you, Brian. Volker?

VOLKER GREIMANN: Thank you. Volker Greimann speaking for the record. Brian, I was raising my hand just for this. I am very much of the opinion that one domain name can be enough if there is certain other information available from experience, such as the naming patterns in the domain name. That makes it appear worthwhile to have that review and search on the platform.

To give an example from standard practice, if a domain name is registered and we treat fake shops like phishing, a fake shop that says "brand name online" or "brand name outlet dash country" suggests a very high likelihood that there will be more because the naming pattern suggests a campaign. Other cases are not as clear-cut or are one-off registrations. It is visible to me from experience that these are going to be one-off registrations because they come through a retail platform or a reseller that is usually very good with dealing with abusive cases.

In other cases, when there is a reseller that has higher rates of abuse than others, we might have a look more easily and more often. From experience, I know there are certain triggers that currently trigger me to do that check. If we can somehow operationalize these soft triggers that go beyond the one domain name, then we have won a lot without sacrificing efficiency. Making the industry better should be our goal. Let's not enshittify our processes to make it easier for abusers to stay online longer. Thank you.

PAUL MCGRADY: Thanks, Volker. I am a free speech nick, so if we occasionally use a funny word, I think we will all survive. Reg, go ahead.

REG LEVY: Thanks. I feel like we are getting pretty far afield of some of the actual language, which includes a reasonability standard. Brian is talking about registrants; Marc is talking about accounts. Each of us has a different business model, so the information we see will be different even between Volker and me with similar wholesale models.

If we restrict ourselves, we are going to get into a position where it is also not enforceable. I think the language provided in a lot of these examples where reasonability is the standard is what we should be going for. I know it feels "woobly" to some people, but it is actually a relatively common term legally. We should not be restricting ourselves to saying "look at all the registrants who have registered the same string." Getting into those nitty-gritties is going to be detrimental to the overall attempts we are making here.

PAUL MCGRADY: Thanks, Reg. Reg is onto something important. Essentially, if we dive into and try to build a matrix of what is a garden-variety malicious domain versus a really problematic one that triggers things, we will be trying to build something that captures all the possible outcomes. When the malicious actors think of something new, it won't be on our matrix.

Reg is redirecting us back to a reasonableness standard as the initial trigger. Let's keep that in mind. Are we going to build the Encyclopedia Britannica of things that can go wrong, or are we going to build a reasonableness standard which basically requires some trust for registrars to act reasonably? If they do not, then whatever we build

needs to give ICANN compliance the tools to have a chat with them about that. Yao, please go ahead.

YAO AMEVI AMESSINOU SOSSOU: Hi, this is Yao speaking for the record. I noticed during the discussion that some of our colleagues were discussing what we need to do rather than what is actually triggering the associated domain name check. Thank you, Paul, for making us refocus. Answering the question, I think we already all agree on point 3.18.2 about when the registrar has actionable evidence that a registered name is used in DNS abuse.

When there is actionable evidence that registered names are involved in domain abuse, then we take action. Actions may vary depending on circumstances. We are tending to make a list of all possible circumstances that might involve malicious domain activities, but that will not serve us in the long run. It is good that we focus more on the language of reasonability of the associated domain and how we define the trigger. Only with credible and substantial evidence that those names are involved in abuses should they be considered. Based on obligations, they should take action regarding those domains involved in such activities. That is what I want to mention briefly.

PAUL MCGRADY: Thank you, Yao. All right. Farzi, welcome back.

FARZANEH BADIEI: Thank you. One thing we need to be clear about is when we talk about reasonably... I am not getting into the territories of what is reasonable.

But from our perspective at the Non-Commercial Stakeholder Group, when we talk about taking action or further investigation, we need to think about the proportionality of that investigation because pattern finding is a kind of surveillance.

If we have to conduct that, it has to come with safeguards. When we say the registrar shall promptly review other reasonably associated registered names, it has to come with qualifiers that this should be done proportionally. I hope we are not prescribing how, but if there are suggestions, it has to be proportional, legitimate, and necessary. We must not hamper or affect innocent domain name registrants that could be in that portfolio of the abuse. Thank you.

PAUL MCGRADY: Thanks, Farzi. Before you go, a clarifying question: are those safeguards and proportionality about the initial trigger, or is it about what they do after that initial trigger?

FARZANEH BADIEI: I believe it is both. We need to be very targeted when we undertake surveillance of an account. Expanding the method of ADC so that it could potentially lead to investigating other accounts could trigger other concerns. I believe it has to be before, during, and after the investigation.

PAUL MCGRADY: Okay. Thank you. All right, we have a healthy queue. I know it feels like we are talking to indecision, but we are not. Staff is gathering all of this

as we go. We are not at a point where we should be wordsmithing the stable but not final language. We need to get a set of principles that we can agree on. If you are relatively new to PDP and feel dissatisfied, that is okay. We are going to get there, but we need to get everybody's thoughts out so that everyone can be heard. This is what we should be doing. Anil, go ahead.

ANIL KUMAR JAIN: Paul, I hope I am audible.

PAUL MCGRADY: Yeah.

ANIL KUMAR JAIN: Thank you, Anil for the record. Quick two things. Number one is that from ISPCP, we suggested that the determination related to the trigger should be restricted to those categories defined in the RAA, which are malware, botnet, phishing, pharming, or spam as a delivery vector. Are we looking beyond this? Yes or no?

Second, I strongly recommend that if a Law Enforcement Agency submits a report or a request for investigation, the registrar must undertake the investigation immediately without thinking otherwise. I understand that there has to be a proper balance between the cost to the registrar as well as to the security aspect of the whole community. Thank you.

PAUL MCGRADY: Thanks, Anil. Anil raised a really interesting question. If there is anybody advocating for a trigger outside of the definition of DNS abuse found in 3.18.2, let's hear from you. I do not know that we have heard that, but it is a great question. Martina, go ahead.

MARTINA BARBERO: Thank you very much, Paul. Certainly, the GAC is happy with sticking to the definition of DNS abuse in the contracts. I wanted to support Brian. He framed the problem in a way that is similar for the GAC. I wanted to offer the GAC perspective on why we try to anchor the trigger in actionable evidence by itself. Maybe the why will give some arguments on how it can be done differently.

Our main concern is that we need to have something that is enforceable for compliance. The more we go towards something that is a suspicion or something on top of actionable evidence, the more we give wiggle room to those who might not want to implement the rules or those who want to avoid doing associated domain checks. We are quite sure most of the community already does these checks, but there might be a few rogue actors that want to try to avoid the rules. We want to be sure compliance is the tool to enforce this policy.

As Reg said, we cannot have a list of all the things that the registrar could look at because registrars have different business models and different data. We cannot have a super detailed matrix, but if we insert something like "reasonable," it needs to be something workable for compliance that does not allow rogue actors to exploit the weakness of the rules. That is why we really wanted to ground this into actionable

evidence as a way to say this is something already understood and can be enforced by compliance.

PAUL MCGRADY: Thank you, Martina. We have Michaela next and then Volker.

MICHAELA SHAPIRO: Thank you so much for the mic. Apologies for my voice; I was at a wedding this weekend and had maybe too much fun. I wanted to echo a few points, particularly from Farzi, related to how proportionality could be particularly useful when we think about what this reasonableness standard could be. I completely agree with Martina about the evidence-based part of that reasonableness standard. Proportionality could be very helpful to understand how you are thinking about reasonableness.

As others have said, the scope is limited on purpose. We are not talking about compromised domains at this stage; that is not our role. My concern here is it is a tricky balance. We need to have a trigger that allows for enough action to address the most problematic cases so you do not have this tumbling effect. At the same time, we do not want it to be so overly sensitive that it could potentially lead to a negative impact on registrants who should not be caught up in these investigations.

We haven't defined what the investigation looks like and what the impact would be on the registrants being investigated. My concern would be that making it overly sensitive would be overly burdensome on those having to do the investigation. You could end up with too many being investigated, being overwhelmed, and jumping to

enforcement action. On the other side, the registrants caught up in this are not... well, I will defer to Farzana to explain the potential risk to the registrant there. This reasonableness standard applies on both ends in terms of how the investigation takes place and the trigger. I will just stop there. Thanks for the time.

PAUL MCGRADY: Thanks, Michaela. Question number one is focused on the trigger event. There will be other discussions down the line about what is next after the trigger. Right now, to get through question number one, we should focus on the trigger events. We have Volker, Marc, and then Brian.

VOLKER GREIMANN: Thank you. I think Paul and Reg are onto something when you say that there has to be reasonableness. Creating a matrix of specific triggers would probably lead us into a path that would date this policy very quickly. Therefore, we should probably go the route that we have gone with a number of other times with ICANN, which is to reference an advisory that would be created and updated on a regular basis by ICANN and various stakeholders.

That advisory would look at those triggers and update what is reasonable to expect, which cases are currently popping up, and which triggers would be expected. Basically, we create an advisory and update that on a regular basis to make sure we stay up to date. That way we can have the best of both worlds: a trigger that works and also a trigger that keeps on working. Thank you.

PAUL MCGRADY: Thanks, Volker. Can I ask a follow-up question: who updates that advisory? Is it ICANN compliance that updates it?

VOLKER GREIMANN: That is a good question. I think there are multiple ways of doing that. That could be a community-led effort from a small working group or team between registrars, SSAC, or various reporters that come together on a regular basis. We are not at that stage to define that yet, but if we could agree on that as a basic principle, I think we have won a lot already. Thank you.

PAUL MCGRADY: Thanks, Volker. Staff, please do capture the idea of a reasonableness standard that operates in conjunction with a reasonableness advisory. Whatever that is, if we can grab that, maybe that is how we bridge the gap between a matrix, which would bring certainty for about three months, and the fuzziness of "reasonable" standing alone without examples or safeguards. Let's see if we can capture that. Marc, go ahead.

MARC TRACHTENBERG: I completely understand the concern that Volker and Reg have raised about the potential cost or the time it takes to do these checks slowing down the investigation of abuse. Personally, I think this is outweighed by the potential of quickly identifying other domain names being used

for abuse. I understand the point they are making, and it is not unreasonable.

I am struggling to understand this proportionality argument that Farzana and others are making because I do not understand what the potential harm is to other registrants or customers of the registrar. If someone reports "chasebanksupport.com" and provides actionable evidence that it is being used for DNS abuse, and that triggers the associated domain name check, the registrar looks for other associated domain names. If they find "chasebankcustomersupport.com" in the same account, that is probably also being used for DNS abuse.

If they also find "praisejesus.com" or "ihatetrump.com" or whatever other domain name is in there making political speech, they are not going to take action because there is no evidence of DNS abuse. What is the harm? This is not the government looking and finding out what every single customer registers at every registrar. This is only the registrar itself doing a quick check to see what domain names are associated and seeing if there is any obvious DNS abuse. I am struggling to see what harm there could be to other customers in that situation. That is where I do not understand this proportionality argument.

PAUL MCGRADY: Thanks, Marc. I know Farzi is in the queue. Let's hear from her on how you would put a proportionality test together when you have one domain name found to be abusive. How do we apply that to one domain name? That is where I am struggling.

By the way, I apologize to Chris, who put a thing in the chat at the beginning and I got distracted by audio troubles. Can people put in the chat if they have any objection to the alternates participating in chat? I don't, but let me know. I am a "more speech" guy, but if anybody hates it, speak up. Brian, please go ahead.

BRIAN CIMBOLIC: Thanks, Paul. I want to circle back on one thing Martina said and one thing Volker said. To be clear, I do support a reasonableness standard, and that is a standard relied on in the registry agreement and the Registrar Accreditation Agreement quite a lot. I view two reasonableness standards. There is one as to how a registrar conducts an associated domain check. I think that is really important because we have heard from our registrar friends how many different business models there are.

An associated domain check for a pure retail registrar is going to look very different from a wholesale registrar where they may have a reseller of a reseller. I think allowing for reasonableness in how a registrar conducts an associated domain check is really important. I have more concerns about the enforceability of whether a registrar conducts an associated domain check. Those are two very different things.

An advisory could really help elucidate how a registrar conducts an associated domain check. A playbook already exists for this: the compliance advisory for enforcing the DNS Abuse Amendments. I will find it and put a link in the chat. The DNS Abuse Amendments say that registrars and registries have to reasonably take action and reasonably

investigate. Rather than having a hard definition of what is reasonable, the guidance comes in the advisory and helps advise ICANN compliance staff as to clear examples. It gives them a North Star on how to enforce. I think that could really be helpful here, but much more on the "how" as to the "whether" a registrar has to conduct a check.

PAUL MCGRADY: Thanks, Brian. That keeps going back to the trigger issue. How do we pull the trigger on that? I have asked Ching to join the queue if he wants to. We have four folks in already and under 10 minutes because we need some AOB time. I will draw the line after Erum, unless Ching jumps in to talk about slow burns. We will finish up our deliberation time. I think this has been great. It has helped us focus on trigger versus what happens after the trigger, and matrix versus reasonableness standard. For those new to PDPs, it may feel like we are not getting anywhere, but we absolutely are. Rod, go ahead.

ROD RASMUSSEN: Thanks. I think Brian just said some stuff which ties into what I wanted to bring up here. It also came up in the chat earlier. First, I want to point out that we really do need to be careful about the language we are using. There was a whole chat discussion about what is "bad." In doing what we are doing, we need to make sure we are talking about maliciously registered domains. That was brought up by a couple of inputs but not necessarily all of them.

We are not just talking about compromised domains, at least where the compromise occurs outside of a registrar account, like at a hosting

platform. We need to be careful as we are developing language because an external reviewer may miss that. Is there a case where the compromise is at the domain account itself, say at the registrar? For instance, somebody phished for credentials and logged into your account. Now they can add domains to a legitimate account or repurpose an existing domain for malicious purposes.

That becomes a maliciously registered domain, but not by the person who originally intended to register it. Where does that fall? That is potentially a gray area that we need to tighten up regarding whether that is covered. Your response to that is going to be different from the trigger. Thinking through the ways these things show up, either directly or indirectly with resellers, and articulating that would be really helpful in making sure we do not write policy that excludes things you want covered. I will hold other things for the mailing list. Thanks.

PAUL MCGRADY: Thanks, Rod. Getting feedback now. I hope that is not the phone because that is all I got. Oh, no. Is anybody else hearing feedback?

JULIE BISLAND: Yes, we are. I just muted your Zoom mic, Paul, so you shouldn't have feedback now.

PAUL MCGRADY: Okay. I must have unmuted myself out of habit. Thank you for that. Rod, good questions. There is a difference between a compromised account versus a compromised domain. I would think that on our

reasonableness advisory, if you notice somebody has a compromised account, that might be something that would trigger a deeper dive. We will capture that in the notes. All right, we have Farzi, then Gabe, and then Erum, and we will spend the balance of our time talking about ICANN 86 planning. Farzi, go ahead.

FARZANEH BADIEI: Thank you, Paul. I think the problem is that we want to define the trigger, but we do not know what investigation action we are prescribing. We are kind of in the dark on what sort of investigative methods we expect the registrars to undertake. Based on the severity of the harm and the investigative action, the concept of proportionality will come up, as well as the trigger and the threshold.

What sort of threshold should we have in order for the registrar to investigate all the one thousand domains of an account that has one malicious domain name? I think we are a little bit unclear because we are not talking about investigative actions. I understand why, because we do not want to prescribe those, but if we want to talk about the trigger, we have to know what sort of action comes next and define it in accordance with that.

We can go through examples. Marc keeps asking what sort of negative impact there would be. We have explained this over and over. Basically, if the registrar has to do some kind of associated domain check and they are not careful, or they just get rid of the account or portfolio, it could have implications for other domains that would not be maliciously registered and are serving people. We have talked about the impact and

given examples. I will put them down and send them to the list. Thank you.

PAUL MCGRADY: Thanks, Farzi. Marc, I saw your hand go up, but I drew the line under the queue after Erum, and we are not going to have time. I wanted you to know sooner rather than later. Maybe you can put that in chat or into the document in between. Gabe and then Erum, and then we are going to spend the rest of our time on AOB related to ICANN 86. Go ahead, Gabe.

GABRIEL ANDREWS: Copy that. This is Gabriel. This is a question mostly intended for Volker, but Farzi's question is timely because it plays into it. She asked what happens if there is one domain that is well-evidenced to have been a malicious registration on a customer account with a thousand other domains. I think what I am hearing from various folks is that there would be an expectation that reasonable investigation would occur, and that standard might be impacted by the facts and circumstances.

You might have a difference between a direct customer of a registrar who is not a reseller, who registered a thousand domains all within the same four-hour period and started making abusive use of one within four hours, versus a reseller customer where this is one domain of a thousand. Volker, if you had a reseller customer and a well-evidenced abuse report for one of their domains, what would you expect would be the reasonable investigation? Would you imagine some of that obligation would pass through to your reseller customer to conduct

additional investigation? Curious how that would work in your view. Over.

PAUL MCGRADY: Thanks, Gabriel. Volker, I know you were called out specifically, but we are not going to have time for a rebuttal. Maybe you can put it in the chat or into the document in between meetings. Erum, go ahead.

ERUM WELLING: Thank you. Erum Welling from SSAC, for the record. I am new to this area, but coming from a technical background, I would suggest that the trigger would include looking at the associated registered names. We cannot be vague; consistency is very important. We cannot decide everything is okay if there are three or less, but not if there are more.

Many times, when there is one malicious action, it could even be a test to see if there is going to be a response. If there is no response, that may be a successful pathway to additional abuse. It is very important to address things as early as possible and get the word out that this is not acceptable. If the reseller has that within their portfolio, it is on them to correct the problem and not let it slide. It is very important in the technology world to identify where the problems are and to address them promptly so the bad actors don't... I do not care if we are using the word "bad." It is a category to indicate something malicious is potentially going on. It is not to categorize the people. I am talking strictly about the activity. The activity is inappropriate. Let's not get lost in the language. It is a matter of identifying something potentially

malicious, resolving it, and making sure it does not spread because there are victims on the other side. Thank you.

PAUL MCGRADY: Thanks, Erum. That was a great discussion. We have three minutes left, and I am going to turn it over to staff to talk about ICANN 86.

JOHN EMERY: Thanks so much, Paul. We will be sure to end on time. ICANN 86 is already around the corner. We are planning on having four DNS Abuse PDP sessions in Seville. Those will be during the standard working days, the 8th through the 11th. During prep week, there will be one prep week webinar to update the community on the progress of this DNS Abuse PDP. Volker, if you have something, do it real quick.

VOLKER GREIMANN: Just one quick request regarding scheduling: please make sure you do not schedule any of our sessions against other very important sessions like council sessions or other abuse-related sessions so we can focus on the topic and ensure everybody is able to attend. Thank you.

JOHN EMERY: Absolutely, Volker. Staff is coordinating across all groups to try and ensure no conflicts. That is a number one priority for us. As an FYI, next steps: we have to confirm the project plan. Those will come out in the notes and action items. It has to be to Council by the 6th. Look at the collaboration tool and provide feedback. Staff will be putting in all of the

comments or suggested language from the early input request. We are going to ideally start working on charter question two, and staff will populate the collaboration document. We will leave it there.

PAUL MCGRADY: Terrific. All right. Thanks everyone. Good call. Please be active on the list and in the documents. If we do that, we will get our work done. If we don't, we won't, and we will have to add meetings, and that sounds sad. All right. Thanks everybody. Happy Monday.

VOLKER GREIMANN: Thanks. Bye.

[END OF TRANSCRIPTION]