JULIE BISLAND: Good morning, good afternoon, and good evening, everyone. Welcome to the DNS Abuse Mitigation PDP1 Working Group call taking place on Monday, 11 May 2026. We have apologies today from Paul McGrady. Statements of interest must be kept up to date. Please raise your hand or speak up now if you have an update to share. All members, participants, and alternates will be promoted to panelists. Please watch your screen for the prompt to be promoted. Observers will remain as attendees and will have access to view chat only.

All documentation and information can be found on the DNS Abuse PDP1 wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name 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. With that, I will turn it over to our co-chair, Nick Wenban-Smith. Go ahead, Nick.

NICK WENBAN-SMITH: Thank you very much, Julie. That was very comprehensive. You can tell by now, given Paul's apologies, you have the reserve team chairing this meeting. Be kind and tell me if there are things you would like me to do differently in the future. I am very happy to take that on board. Today's meeting is the usual 90 minutes. I will try to finish exactly on time, if not earlier. You can see here how we have planned the time allocation for the meeting.

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.

Is there anything else anybody wants to raise with me now in terms of the timing? In particular, if there are additional areas of business I need to factor in, that would be nice to know before we start. I see no hands raised, but I will keep an eye on things. This timing is something we will try to stick to, but as ever, this is your collective PDP. If we need to spend more time on some things and less on others, I am perfectly prepared to be flexible about that.

We set out here a forward plan. People who have been on working groups or policy things with me before know I like to have a forward-looking waterfall as to what is coming up, particularly with ICANN 86 looming quite quickly now. You can see here the draft. Here we are carrying on the deliberations on CQ 5 and 6. We thought we would look at the straw person language next week. The week after that, we will review the language of the first six substantive parts of it to look at it as a collective set of CQ language. None of this is fixed, but we are trying to see whether there are areas where the first six questions collectively hang together as a coherent set of policy statements.

Then we will try to go through the final CQs 7 to 9, which tend to be more procedural. The aim is to have gone through all of the questions at least once and reviewed the language of the substantive part before we get to the working sessions in ICANN. We will plan the schedule of the ICANN working sessions a bit closer to the time, depending on the progress made over the next four weeks. Ideally, I would like to have some good face-to-face time to thrash through the language and make a lot of progress. These four weeks leading up to that will put us in the best position possible for the ICANN working sessions together. Are there any questions so far? Thank you, Brian.

The slides change without me having to do it. The staff are amazingly telepathic. This is just a reminder that it feels like a long time since the PDP started. The key principles are to get something which can be adopted by the Board, receive Council support, and solve the questions as laid out in the Charter. I think we all understand that this is supposed to be a lean, narrowly focused PDP with very specific questions. We should try to stick to the roadmap on that front and be kind to ourselves. There are lots of other interesting questions which I would really like to explore, but that is not part of the PDP today.

When reviewing the straw person task, ask yourself: Can my group live with this recommendation? The ask from us is that if there are issues and concerns, it is really helpful to articulate rationale as opposed to just saying you do not support it. Reasons why you do not support it and clarifications are helpful. From my personal perspective, it is not so much if you cannot support the recommendations, but if you think they could be improved or clarified. This is a hive mind of collective expertise here. We can move forward. This is a fairly obvious recap of what I was just saying.

For CQ5, thank you to everyone for putting feedback into the Google comment document. There were many rich points in there. This is the question which I think we all understand. There is an implication that there is an adverse impact on innocent domain name registrants in terms of false positives, but that is just my interpretation. We received a variety of inputs. The GAC noted that remedies are outside the scope of the PDP. The IPC and others said that remedies questions are already coming up in the base RAA as it already exists, so we do not need to do this. There are further questions around potential harm for registrants

and the right remedy in that case. It is inevitable that there will be false positives, so it is a really important question to explore. I will open the floor for thoughts. Farzaneh, Martina, Marc, and Mary are in the queue. Farzaneh, the floor is yours.

FARZANEH BADII: Thank you, Nick. Hello, everybody. This is the first time I have heard my voice this morning. NCSG decided in its preliminary response to feedback that remedy is very important for us. For the past two years, in every DNS abuse session, we have mentioned that if we have mitigation mechanisms for DNS abuse, we need remedy in cases of false positives and other impacts. We wanted to provide a more complete response, which is why we did not respond to the question. We do not agree with our colleagues in GAC and the Commercial Stakeholder Group that remedy is out of scope. We believe that wherever we come up with a policy that could have potential impact on the domain name registrant and the end user, there should be avenues for a remedy to be predicted. It is a normal policy development principle.

If the argument is that remedy is provided by the RAA, then please point us to those paragraphs and we should discuss them. We should see if they are sufficient and mention them in our work as well. My colleague, Michaela, sent an email with our suggested text for remedy. If we could give her panel access so that she can weigh in on this, that would be great.

NICK WENBAN-SMITH: Brilliant. Thank you. Farzaneh, just to clarify, it is not a remedy to the check being done itself. It is a remedy if there is a check done as a result of the ADC and then there is mitigation action taken which was inappropriate in that context. Is that clear?

FARZANEH BADII: Yes. I see that Brian is raising this point in chat. If there are unintended consequences for the domain name registrant, this could involve accessing their data or suspending their domain name. I understand that you keep wanting to say that enforcement is different from the ADC, but we think there should be some discussion about remedy and what will happen if things go wrong.

NICK WENBAN-SMITH: Presumably, currently, if a registrar wrongly puts a server hold on a domain name, the registrant gets in touch with them and they reverse it. Are you trying to make that more formal? I am trying to clarify your point.

FARZANEH BADII: We want to have that. We also want to discuss other potential impacts that could happen to the domain name registrant. I appreciate if we could have a conversation about that. If we cannot come up with any kind of impact, then we can move on, but I think we should allocate some time to discuss it. Thank you.

NICK WENBAN-SMITH: It would be helpful if you could be more precise. When I have thought about this, the only thing I can think of is a mistaken suspension of a domain name which needs to be reversed. If there are other things in terms of damage to domain name registrants, then we need to be clear about what those could be so we make sure they are covered adequately. I will move on in the queue now, but please think about that point. Martina, you have been waiting very patiently. Your turn is next.

MARTINA BARBERO: Thank you very much, Nick. Thank you, Farzaneh. I wanted to clarify the GAC position. The GAC does not view the question of remedies as something of no importance. On the contrary, we think this is an important matter. What we are looking at with this PDP Charter is Associated Domain Checks. We are still struggling to understand the harm linked only to the ADC, rather than the mitigation action that results from it. The mitigation action, such as suspension of the domain name, is carried out if there is evidence of abuse. A registrar can be mistaken, but the suspension is not per se a consequence of the ADC. The ADC triggers an investigation that leads to suspension if abuse is found.

At some point, you kindly suggested that the NCSG provide scenarios of how an ADC in itself can cause harm. We are open to discussing remedies to the ADC itself if there is harm caused simply by the ADC. We are also open as a GAC to have a larger PDP on remedies, because the question of unfair or unjust suspension is broader than what is linked to an ADC. We do not think it works to say that if a domain is

suspended because of an ADC, one wants a remedy against suspension in the context of this PDP. It is a broader topic. We need to be evidence-based and identify the harms linked to an ADC specifically. If we do that, then we might be able to discuss remedies more specifically. At the moment, we are still confusing mitigation and the ADC. The remedies to the ADC are still unclear because we do not really understand the harms for the ADC only, not the mitigation.

NICK WENBAN-SMITH: Thank you very much. That is a very clearly made point. I completely understand the distinction between performing the ADC itself and other broader aspects of mitigation. If you have your domain name suspended, you would not necessarily know whether it was because of an ADC check or an abuse report. The avenue to a reversal needs to be taken in a broader context than purely the ADC. Marc, I think you're next.

MARC TRACHTENBERG: Martina made most of the points that I was going to make, and she made them clearly. I see Farzaneh is responding in the chat, so I will respond to that. Again, the ADC and suspension are separate. Farzaneh says that the suspension distinction is mythical, but it is not. The comment that some registrars will suspend entire accounts is speculative. To Eberhard's comment, they do that at their own peril. Right now, the ADC only identifies domains that are likely to be related. No registrar I know would reasonably, and in compliance with the

contract, take action against another domain name simply because it may be related to a domain used for DNS abuse.

They would only take action, at least as permitted by the contract, if there was actionable evidence of DNS abuse or some other breach of their terms. The separation is not mythical; it is real. Currently, a registrar could suspend a domain name in response to an abuse complaint or for another reason, and there are remedies. The registrant can alert ICANN Compliance to the fact that the registrar is not in compliance with their obligations under the agreement and ICANN policies. ICANN Compliance will investigate this. The remedy already exists. Unless we can identify some type of more specific harm that results from the ADC, I think we need to move on from this topic. If there is identifiable harm, it should be addressed. But that harm has yet to be identified. We cannot spend more time on speculative or phantom harm, especially in the limited context of what the ADC actually is.

NICK WENBAN-SMITH: I got the point. That is well-stated for the record. Brian is next. He is probably going to give us a lesson in the RAA remedies which exist already.

BRIAN CIMBOLIC: Nick, you know me too well. Both things can be true. There is no recourse mechanism set forth in the RAA. Currently, if a registrant has its name suspended for DNS abuse, there is no section of the RAA they can avail themselves of to try to provide evidence to the registrar that they got it wrong. While I think that is a worthwhile initiative and effort,

PIR is one of the few contracted parties that actually maintains a formal recourse process to include appeals to a neutral third party. I support the substance, but I do not support the process here.

From the beginning, this PDP was narrowly tailored. We are here to get a specific job done. Recourse for mitigation of DNS abuse does not currently exist. Why would we have something that is a subset where only registrants impacted by an ADC have a recourse mechanism, but registrants that are not related to an ADC do not? It does not make sense. It feels like we are trying to take a new policy initiative and push it into this narrowly scoped PDP. If we all bring our specific passion interests to this and try and force them in where they do not fit, then this PDP is going to go on forever. I do not support this here. I support recourse mechanisms, but I view this as outside the scope of this PDP.

NICK WENBAN-SMITH: I understand that being a registrar is a competitive business. Presumably, registrars are competing to treat legitimate registrants well and not suspend domains wrongfully. Customer satisfaction is important in the gTLD registrar world, as it would be for a ccTLD as well. Eberhard, you are up next.

JULIE BISLAND: Eberhard, we are still unable to hear you.

NICK WENBAN-SMITH: Ching, you are next. I will come back to Eberhard if we can sort out the audio.

CHING CHIAO: Thank you, Nick. This is Ching from the BC. The BC would support what Brian and Marc were saying. However, we still need to address this Charter question regarding what the corresponding remedies would be. From the BC point of view, the ADC is just an ADC and there is no mitigation for this particular PDP. But if a portfolio registrant has a name labeled as an ADC by another group wrongfully, and subsequently that group gets suspended through other processes, that wrongfully conducted ADC is the cause of that potential takedown. Therefore, I think there should be proper remedies placed here because of that wrongfully labeled ADC in the first place. Thank you.

NICK WENBAN-SMITH: I understand the domain suspension following the ADC having an adverse impact, but the ADC in of itself is a much narrower point. It is difficult to see a registrar looking at its own data and abuse reports as anything other than legitimate, prudent checks to see that their infrastructure is not being abused. Eberhard, can we hear you now?

EBERHARD LISSE: Let me try now. I had to re-plug my cables. I am a great friend of natural justice and the principle that the other side must be heard. However, I agree that mitigation in itself is a separate issue. The harm caused by mitigation is out of scope. Nothing prevents us from reporting to the GNSO Council that we have identified an issue with their mitigation process. We can say we noticed there is no remediation process and ask the Council to take it on board. We can discuss whether an ADC itself

has an adverse impact. If we come to the opinion that this is possible, then we must discuss a remedy. If we come to the consensus that the check itself is not causing harm, then we do not need to discuss it. We should start at the beginning and see what the ADC actually does and if there is harm there. You can inform someone of what was seen and ask for their position.

NICK WENBAN-SMITH: I am trying to work out how a registrant would even know if a suspension was due to an ADC or an abuse report unless they had inside information. Reg is the registrar who already does ADCs and can probably tell us if they are experiencing complaints. Reg, you are next.

REG LEVY: The RrSG addressed in our response that there are already mechanisms. They exist within the terms and conditions of each registrar, which can be as strict or as customer-friendly as the registrar and its customers agree. It is also in the registrant benefits and responsibilities that exist on the ICANN page. Regarding the harms of the actual ADC itself, the RrSG conducted a data privacy impact assessment in public at the Contracted Party Summit and determined that evaluation of personal data could be a relevant harm under certain international laws. However, the purpose outweighs that harm. This is a valid point the NCSG is raising and one that has been addressed by the RrSG. I encourage people to take a look at that document.

NICK WENBAN-SMITH: Thank you. I listened to that session on the data impact analysis, and it was interesting. Michaela is next in the queue.

MICHAELA SHAPIRO: Thank you all for this substantive discussion. I do not want to beat a dead horse. We may be arriving at a point where we agree to disagree on certain elements. Nick, you made a helpful point that when it comes to mitigation action, you may not necessarily know where it came from or whether it resulted from an ADC or some other investigation. That is the crux of the issue for the NCSG; there is a lack of transparency around these processes. There are cases where you cannot give full detailed notes for safety reasons. But we want to emphasize that there is a potential for harm. It would be helpful to hear more from Reg about how they concluded that benefits outweighed the harm.

These investigations differ based on business model and the type of abuse being flagged. It is still unclear what the investigation would entail. From a data privacy protection space, there seems to be convergence in the group already that there could be potential harm associated with the scope and scale of that investigation as part of the ADC. Perhaps coming back to Q4 around data protection safeguards would be a compromise avenue. We want to make sure that is strengthened. I also want to flag to the GNSO that this is a priority issue to talk about recourse when it comes to DNS abuse mitigation. If we do not discuss it here, we are concerned it will never come back. We do not want it to be sidelined from future discussions.

NICK WENBAN-SMITH: It is very difficult because registrars form contracts with registrants all over the world. From a UK or EU data privacy perspective, if you have been alerted that a set of domain names has been criminally made, there is a legitimate basis for processing data to check for other examples. It is difficult to legislate for that worldwide under all different laws through this PDP. I am worried the question is bigger than the ADC-specific questions we started with. The points are well made and will be put into the record, even if they are not part of the ultimate policy wording. Reg, you have your hand up.

REG LEVY: Thank you, Nick. Michaela, thank you for raising your concerns. A base assumption in our DPIA was that it was against a maliciously registered domain, not a compromised domain. The registrant information is not that of an innocent registrant. Starting from that baseline assumption, we can weigh the benefits of looking for additional information against the harm already caused to the broader internet. If it were a compromised domain, there might be a different outcome. Because we are starting from the fact that it is a malicious domain, reviewing for additional harm is typically already in the reasons a registrar can use your data. When you agree to a service, one of the reasons the registrar can use your data is to combat fraud and malicious use. That is disclosed to the registrant and is part of the information they already have.

NICK WENBAN-SMITH: I understand, but there is no ICANN requirement that registrars must have those specific data privacy explanations. You are governed by the

laws of the territories you are in. Most places I am familiar with do require assessments. It is a complicated question to mandate something that might conflict with national legislation. We move on to Charter question number six: What are the appropriate timelines and thresholds for initiating and concluding the Associated Domain Check? If your ADC uncovers evidence of abuse, that should be a trigger to act promptly according to existing registrar obligations. There is a divergence around what an appropriate check would be. The NCSG mentions disproportionate action and the investigation fitting the evidence. Can we come up with specific time frames? The BC advocates for a mandatory 24 hours. The IPC suggests 72 hours, mirroring data breach deadlines. Brian and Volker are in the queue. Brian first.

BRIAN CIMBOLIC: The RAA DNS abuse language uses the word promptly. The advisory that ICANN Contractual Compliance put out for the DNS abuse amendments says that what makes an action prompt will vary depending on specific circumstances. It is impossible to prescribe a fixed amount of time. Instead, registrars must demonstrate ongoing attentiveness to allegations commensurate with the potential harm. What I do not want is a disjointed system where the standard is promptly for actual mitigation under the RAA, but 48 hours for the ADC. I encourage everyone to read the language in the advisory to see if that context makes sense to them.

NICK WENBAN-SMITH: I heard that the wheel has already been invented and we should not try to overcomplicate things with a different timeframe over the existing prompt wording. Volker.

VOLKER GREIMANN: I agree with Brian. Even a malicious registrar would be hard-pressed to argue to Compliance that promptly means something different for an investigation than for an ADC. This discussion misses the point of how registrars operationalize their obligations. We have a high interest in making sure processes are efficient. Most of us will do the ADC at the time of the investigation of the domain name as part of that investigation. We want to do that as soon as we complete the ticket. If someone suggests a 48 or 72-hour timeframe, it does not really play into how we work. We perform the ADC to get rid of the ticket and move to the next one.

NICK WENBAN-SMITH: So you perform the ADC at the same time you receive an abuse report?

VOLKER GREIMANN: When we receive an abuse complaint and there is some point to it, we perform the ADC as part of the investigation. The fact that multiple domain names are engaged in the same activity is part of the evidence package we use to identify the abusive nature of the first domain name. The ADC is part and parcel of the investigation for those registrars already engaged in this.

NICK WENBAN-SMITH: That is super interesting. You will not have to change policies because it is already wrapped up in the initial investigation.

VOLKER GREIMANN: Correct. That was part of the initial thought process. We wanted to enshrine processes that already exist and raise the floor so everyone is brought to the same level.

NICK WENBAN-SMITH: Since this is existing best practice, is there a way of encapsulating that in the recommendations?

VOLKER GREIMANN: It is difficult because every registrar will have different approaches. That is why we have looked at a principled approach rather than a descriptive one.

NICK WENBAN-SMITH: Gabriel, you are up next.

GABRIEL ANDREWS: This is Gabriel Andrews. In responding to this question, the GAC had contributions for both initiating and concluding the Associated Domain Checks. Regarding the initiating timeline, we believe checks should be initiated when the registrar has actionable evidence that a name has been used, is being used, or is likely to be used for DNS abuse. Echoing Brian, the GAC points to the existing contractual requirement that a

registrar must promptly take appropriate mitigation actions. It seems reasonable to apply that across the board to all domains associated in that abusive activity. It is very important to give ICANN Compliance the flexibility to determine what is appropriate. The GAC also focuses on whether DNS abuse can be prevented prior to domain delegation rather than purely reactively.

NICK WENBAN-SMITH: If you were an outside observer, you would be surprised that registrars did not already act promptly on abuse. It is good business sense to minimize infrastructure abuse. We are trying to lift the baseline so that external observers think we are doing a responsible job. Eberhard, you are next.

EBERHARD LISSE: I like promptly. We should not be over-prescriptive or put a fixed timeline shorter than what is currently used in Compliance. We should consider that not every registrar is as well-organized as huge ones. If it is a manual process, a small registrar might find it a big cost factor if they have to do it immediately. If you show Compliance you are doing your best and acting, that is what promptly means to me.

NICK WENBAN-SMITH: I see a lot of agreement over the use of promptly. Ching, the floor is yours.

CHING CHIAO: The BC will not be able to accept promptly simply because we are addressing this issue for registrars outside of this room. Promptly would not work because it gives them a vague measurement without a proper timeline. We have seen registrars or registries doing ADCs for sales and marketing rather than just abuse purposes. Within a reasonable period, you should be able to capture an ADC and put it aside for if an abuse case happens. Prompt is not concrete enough for those with bad intent.

NICK WENBAN-SMITH: I want to test the consensus. Advocates for prompt language say it gives flexibility. For complicated investigations, you might need a week. We do not want people to think a week is the deadline if they could do it in three hours. A serious phishing attack should be mitigated in minutes. If you pick a single timeframe, it might be too long for many cases. There are practical difficulties in coming up with a single number. Yao, Marc, Farzaneh, and Jothan are next. Yao, please.

YAO SOSSOU: I support keeping the timeline flexible and tied to the word promptly in the RAA. Different cases of DNS abuse present different challenges in terms of urgency and complexity. Registrars operate under different business models. The ADC deadline should remain risk-based and evidence-driven. Fixed deadlines can unintentionally incentivize rush mitigation and over-association, which increases false positives. Flexibility is key to ensuring effective action against well-evidenced DNS abuse. The threshold should remain tied to actionable and well-

evidenced abuse under the RAA Section 3.18.2 rather than predicting future abuses.

NICK WENBAN-SMITH: We should not start from a blank piece of paper. Short timeframes could have unintended consequences of over-mitigation. Marc, then Farzaneh.

MARC TRACHTENBERG: A time limit like 72 hours does not prevent registrars from taking action sooner when appropriate. You could use language like promptly, but in any event within a certain timeframe. Promptly is problematic because it is not clear what it means, and different registrars have different ideas. In this context, there is no transparency. A reporter of abuse will never know if the registrar took action. There is no way to report it to Compliance. I do not know how ICANN is going to determine compliance other than with rolling audits. Without a standard, those audits are not practical. An obligation without a way to determine compliance is meaningless.

NICK WENBAN-SMITH: Could language like promptly, but in any event within 72 hours, lead to mitigation being delayed if people think they have the full 72 hours?

MARC TRACHTENBERG: It cannot be any worse than having no deadline and leaving people to their own devices. Good actor registrars want to act promptly for the

safety of their networks. Having a limit should not affect them. There is more risk in having a vague promptly with no limit whatsoever.

NICK WENBAN-SMITH: We should think about how this can be an implementable policy capable of being adopted by the Board and policed by ICANN Compliance. Farzaneh, then Volker.

FARZANEH BADII: I want to discuss thresholds. If we are starting an ADC on only one report of abuse, we need to look at how we bring proportionality to the threshold. For example, if there are reports on a portfolio about Telegram-related domains being used for scams, are we going to restrict it to the keyword Telegram, or look at the whole portfolio? Are we talking about a threshold of a certain number of domains?

NICK WENBAN-SMITH: If someone registers 1,000 Telegram domains in a few minutes, that is unusual. If you get one report, you would look at the whole sequence of registrations as a collective part of the same scam. Ideally, you would take mitigation action before more reports come in. In practice, we want a policy to stop bulk malicious registration campaigns. Volker, you are next.

VOLKER GREIMANN: I was taken aback by Ching saying the BC would not accept promptly. We should look at a constructive process rather than arguing for

months about terminology. Is having nothing better than accepting promptly? Promptly is a defined term in the RAA that has been employed effectively.

NICK WENBAN-SMITH: Someone will have to compromise because we cannot all get what we want. We want a policy in a reasonable period of time. Perfection can be the enemy of the good. We know what the issues are, and talking about them for another two months will not give us more insight. We need to find what is good enough to get through consensus. Jothan, then Ching.

JOTHAN FRAKES: We must be cognizant of the five-day add grace period at the start of a registration. After five days, registries and ICANN keep the fees. A registrar is financially motivated to take prompt action in that first five-day period. We should not take away their ability to do that. Upon detection of malicious activity, there is an immediate review across multiple domains to reduce commercial impact. We want to ensure registrars are not limited in their ability to conduct these checks.

NICK WENBAN-SMITH: We want something that helps registrars and makes domain names safe and desirable. We are in favor of industry-generated solutions rather than governmental regulation. Ching, next.

CHING CHIAO: We are asked to respond to specific timeline questions, which is why we provided a number. We want to ensure there are concrete steps for registrars outside this room to follow. During the upcoming FIFA World Cup, we will likely observe a large volume of related names. Some are individual and some are part of an ADC. It is reasonable for most registrars to follow a confirmed case and trigger the ADC within a certain period.

NICK WENBAN-SMITH: You do not know the reasons for a domain registration until it is used. If a domain is definitely used for phishing, then associated domains should be treated with caution and investigated. Swift mitigation is better than slow mitigation. We will see if there is a consensus, but there is not currently unanimity from the BC and IPC. We will look at potential wording and bring it to the group next week.

We are also asking everyone to look at existing straw person language for the first four Charter questions. Next week we will review the glossary of terms and the collaboration document to ensure we are talking about the same thing. We have 10 minutes back. Thank you to the staff for moving the slides telepathically. See you next time.

JULIE BISLAND: Thank you, Nick, and thanks everyone for joining. This meeting has concluded.

NICK WENBAN-SMITH: Thanks.

[END OF TRANSCRIPTION]