JULIE BISLAND: All right. For the recording, this is Julie Bisland. Good morning, good afternoon, good evening. Welcome to the DNS Abuse Mitigation PDP1 Working Group call, taking place on Monday, the 13th of July, 2026. For today's call, we have apologies from Dennis Tan, RySG; Volker Greimann, RrSG; Steinar Grøtterød, ALAC; Claire Craig, ALAC; and Yao Sossou, NPOC. Alternates joining are Chris Disspain, RySG; Theo Geurts, RrSG; Eunice Perez, ALAC; and Christabel Mebaghandu, NPOC. Statements of interest must be kept up to date. Please raise your hand or speak up now if you have an update to share. Gabriel?

GABRIEL ANDREWS: Yeah. Not an update for statements of interest, but an alternate that I thought had been communicated to you. Our rep, Martina, is out both this week and next, and Janos is joining in as the alternate for the weeks.

JULIE BISLAND: Perfect. All right. Thank you so much. All right. Members, participants, and alternates will be promoted to panelists. Please watch your screen for the prompt to be promoted. Observers will remain as an attendee and will have access to view chat only. All documentation and information can be found on the wiki space. Recordings will be posted shortly after the end of the call. Please remember to state your name before speaking for the recording. And 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 over to our chair, Paul McGrady. Please begin, Paul.

PAUL MCGRADY: Thank you, Julie. Good morning, everybody. Welcome to our Monday mornings together. We have a packed agenda today, and we will go ahead and get started. But before we move to the PDP updates, just wanted to say something at the 30,000-foot level, which is now we're into the details of essentially finalizing the work that we've done. And in details, there can be minutiae. We may be haggling over where a semicolon goes or tweaks to language. And maybe it's not as exciting as solving the problem as it is refining the answers. So I just encourage everybody to stay patient with each other and to stay in the weeds. And yeah, what kind of leadership pep talk is it to say that it might start to feel a bit like a grammar slog? But grammar slogs are important, so let's all stick together and get this done.

So anyways, off to PDP updates. This is our July. Week of July 13th, that's us. We're resolving the remaining pending discussion item. And we are going to do a second read of the initial reports and the assessments. Thank you all who took the time to put in comments, especially on the initial report. There's some interesting and good stuff in there. If you made a comment, you'll be called upon to talk about it, so get ready. Next week, we'll do a third read of the initial report and the assessments. And we will continue to make adjustments as needed. The week of July 27th, if we need a fourth read, in other words, if next week we're not pretty much locked in, we will have the meeting of July 27th. If we don't need it, we won't have it. We won't have meetings just to have

meetings, but if we need it, we'll do that. Week of August 3rd, essentially final read through, final adjustments, and then the week of August 10th through a bit of time there, there'll be a consensus call on the initial report, and we will get that thing launched to public comment. So that is the timeline. We have made great progress, and we're making great progress, so that's good.

We're going to take a few minutes here to resolve the last remaining item. This is one where we've spent quite a bit of time on this one, and we need to figure it out. So, let's do that now. We have the proposed language from the IPC here that has been essentially stable for some time. The only question was whether or not, frankly, the hard-fought-for bullet saying registrars should remain responsible should come out because it's redundant. But I think that was a comfort item, even if it is redundant. And so there's been back and forth on this. Unless the registrars and the IPC have worked this out behind the scenes, leadership team has a proposal to go over that we hope threads the needle. But before we do that, any updates from the registrars or the IPC on any work that might have been done off call? All right, Marc, go ahead.

MARC TRACHTENBERG: Unfortunately, no update. I think we're kind of at a stalemate here.

PAUL MCGRADY: All right. Well then, we will put forward the leadership team's proposed synthesis position to see if maybe we can get some takers on this. So this is what we propose, and the new language is in red. You'll see that

we are saying, "For purposes of this recommendation, information reasonably accessible to the registrar includes information ordinarily accessible to the registrar through its contractual obligations, technical systems, and abuse handling process." So that is proposed to be in the recommendation and in the implementation guidance. We dive deeper. The categories of reasonably accessible information identified in recommendation number three establish the minimum baseline for a reasonable investigation. The recommendation does not prescribe how registrars should review, prioritize, or weigh that information, recognizing that registrar capabilities, technical systems, business models, and the facts and circumstances of individual cases may differ. So this was sent out last week, late in the week, for consideration, and I am hoping that we can get a queue on this. Is there any reaction to this? Does this solve the problem? Is this sufficient for the IPC in terms of certainty? Is it sufficient to the registrars in terms of comfort, and can we move forward with this? If not, is there something in here that can be tweaked to move forward? I'd like to open a queue on this. No reactions? All right, Marc, go ahead.

MARC TRACHTENBERG: I'm still processing this because we haven't had a chance to review this before, but this is definitely better.

PAUL MCGRADY: Yeah. So Marc, yeah, this was sent out on Friday. I know that's not a ton of time, but it's some. If you're not ready to speak to it, it's okay. Why

don't you take a few minutes now? We'll hear from some other people, and then we can hear from you again. Theo?

THEO GEURTS: Yeah, thanks. And this is Theo, for the record. Speed reading here. It looks in pretty good shape, I think. I don't see any red flags going up here, so I think we got some progress here. The last two bullet points, a registrar may rely on a Reseller. You got to be careful with that. Sometimes the Reseller is a criminal, so you don't want to show all your cards there. But yeah, good shape. Thanks.

PAUL MCGRADY: Thank you. Natalie?

NATALIE HOWATSON: Hey, Paul. Natalie, for the record, for the registrars. So we took a quick look at this in our meeting on Friday and are broadly okay with it. We might have a tweak or two maybe a bit later today that we want to put in the document if this makes it in there, but overall looks good for us for now.

PAUL MCGRADY: Terrific, Natalie. Thank you for that. Farzi?

FARZANEH BADII: Hi, Paul and everyone. We are good with this language.

PAUL MCGRADY: Fabulous. Okay. So we have three saying looks good, might tweak, but still looks good. Marc says it looks better. Marc, do you want to come back to it? All right, Marc, go ahead.

MARC TRACHTENBERG: Yeah. I think this seems like a reasonable compromise. This is definitely better than where we were before. It's not, I think, perfect, but no one's going to get everything they want. So this is a significant improvement to where we were.

PAUL MCGRADY: Perfect. Well, great. So it sounds like this threads the needle. We'll hold this queue open for another minute or so. Theo, is that an old hand? All right. Well, I'm not going to belabor this to the point where our happy moment falls apart, so we will move this into the document, and keep it moving along with the other draft recommendations and preliminary guidance. So, terrific.

All right. Now for the grammar slog. The draft initial report. So hold on a second. My handy dandy, beautiful, lifelong spouse has— Thank you.

LISA: You're welcome.

PAUL MCGRADY: Brought me the wrong thing, but that's okay. That's okay. That's not the microphone. But thanks. That's okay. All right. So if I phase out, we'll figure it out. Sorry, Lisa. Yeah. It's that speakerphone I bought. That speakerphone microphone thing. Yeah. Okay. Oh, well. Sorry about that, everybody. So, right. Where were we? Review the initial report.

So I'm going to just run through a couple of slides here, and then we're going to go to the report document itself and just run through the comments. But a few things. While going through the initial report draft, we noticed some non-substantial updates and inconsistencies that we wanted to make that would clarify what we were trying to do. So we've put bullet points in. Reseller is not capitalized throughout the text. Reseller is a defined term under the RAA, so we should capitalize it along the way that we have been doing. On recommendation three, we see available still popping up from time to time instead of accessible. So, I think to be consistent, we will match that language. Reasonably accessible. We have the word registrant used throughout the report pretty consistently. The RAA calls that person the Registered Name Holder, so we thought it makes sense to make that consistent as well since the defined term. In Recs two and four, a reasonable investigation should remain distinct from, we said enforcement, but we think that means mitigation, as opposed to enforcement. So those are examples.

We have a couple of other things. We think we need to add the definition of promptly into the glossary for external users to better understand what we were up to. And so we've taken that from the ICANN advisory that we've all essentially based that on. Promptly means within a reasonable time, under the circumstances, and without unreasonable delay. There is no fixed deadline for what constitutes

prompt, as the appropriate timeframe depends on the specifics of each case. A single universal deadline would inevitably be too long in some situations and too short in others. So that's from the guidance that we've been talking about. So that makes sense to us. There is an RAA reference in preliminary recommendation one. It currently reads in a way that the phrasing implies that DNS Abuse is defined at 3.18.2, when in fact it's in 3.18.1. And so we suggest updating that to where we're referencing the correct part of the RAA. Before we move on, Gabriel, your hand's up. Go ahead.

GABRIEL ANDREWS: Thank you, Paul. Just a clarification question in terms of how these edits are being made, and I'm agreeing with some comments in the chat that these seem like reasonable things to do. But as these edits are made, I want to confirm that we are going to track changes just so we can see them before they are, I guess, finalized. Is that correct, sir?

PAUL MCGRADY: Yes. If they're not already made, they'll be made into the draft recommendation doc— the draft report, rather, that we're about to go through.

GABRIEL ANDREWS: Copy that. Thank you, sir.

PAUL MCGRADY: Yep. All right. So I guess the question is, any concerns about having these in? I don't see anybody raising a hand to object, and I think that most people are saying, "Sounds good," in the chat. All right. Okay, now for the fun part. And guys, there's just no way around it. And so we are going to jump in here and just go through proposed changes. I know our screen says 2.1, but I see Trachtenberg changes in the executive summary. And so, what we're going to do here is have whoever added a comment sort of speak to the comment, say what problem it's solving, why the change should be adopted by the working group. And instead of me calling for a queue after every single line item, because there's a bunch and some of them are small changes, if there's something that you want to say about any of these things, if you can get yourself in the queue as fast as possible so that we're not jumping back and forth from page to page and comment to comment, that would be great. And if we can, in the document that's viewable now by everybody, if we can go back up to the executive summary, scroll back up, we will get started. And Marc, you're on first.

MARC TRACHTENBERG: Sure. So these changes, they're just kind of minimal changes, but the first one talks about threat actors registering large portfolios. They're not necessarily large portfolios, they're just portfolios consisting of maybe multiple domain names that are used for abusive purposes. Let's see. All the domains are not necessarily being used for a single coordinated campaign. These bad actors often have multiple campaigns working in tandem that are maybe not doing the same thing, but are similarly being used for abusive purposes. Going down to 56.

PAUL MCGRADY: Why don't we pause? Yeah.

MARC TRACHTENBERG: Sure.

PAUL MCGRADY: I'm sorry. Go ahead. 56. Sure.

MARC TRACHTENBERG: These are all kind of related, but then going down to 56. The initial language talks about part of an identifiable campaign. I don't know necessarily that the domain names have to be part of a single identifiable campaign. But if you're looking at a portfolio or you're doing your ADC because you see this first abusive domain name that triggers it, and you're looking for domains that might be related, they don't necessarily have to be part of the same campaign. Right? So there could be, for example, a number of domain names targeting one brand and a bunch of other domain names targeting a different brand and a different scheme. If the registrar comes across that, those are still related. The registrar presumably should still take mitigation action if it meets the requirements in the RAA, but it doesn't have to be for part of the same identifiable campaign. We're just trying to identify additional abusive domain names that are related, whether it's part of the same scheme or not. Yeah.

PAUL MCGRADY: Okay.

MARC TRACHTENBERG: I'm kind of making my point in the chat. We're just trying to find additional abusive domain names. Nowhere in the ADC does it talk about, in the charter, finding additional abusive domain names that are used for the same scheme. That's putting a lot of additional work on the registrar as well. They're supposed to determine it's all the same scheme?

PAUL MCGRADY: Got you. Okay. Those are the comments on page three. Let's do a queue. Any objection to Marc's changes?

MARC TRACHTENBERG: I think Reg is agreeing, but I can't tell.

PAUL MCGRADY: All right. Reg, go ahead.

REG LEVY: There's just a lot of magical thinking that's going on here. I really don't understand what we are being expected to do or understand or infer or read the mind of, but I suppose we will be held to it.

PAUL MCGRADY: So, Reg, how do we address your concern? What's the textual change that is causing the concern?

REG LEVY: I think all of these textual changes allow us to make assumptions that may not be based in any kind of evidence. We are no longer to look for associations between domains.

PAUL MCGRADY: Okay. Marc, your hand's back up. Go ahead, and maybe you can respond. We're at the point of textual edits, so if anybody has a textual edit, a proposed textual edit. We've heard from Reg, doesn't like the changes, but would love to have more detail about why or what needs to be tweaked. But Marc, go ahead.

MARC TRACHTENBERG: Reg's point is part of why I made the change. This is so the registrars don't have to read tea leaves or read minds. Right? The existing language made them do that. They have to determine whether it's part of an identifiable campaign or somehow other things are common schemes. The point of this is that's irrelevant. The only thing that is relevant here is if there's other associated domain names, right? And if there are, and they're being used for some abusive purpose, then presumably the registrar takes action. But this, I think, is aligned with Reg's comment and is reducing the need for registrars to have to determine whether there's some common scheme or not, because

that's not relevant. It's only relevant whether other domain names are being used for abusive purposes.

PAUL MCGRADY: Thanks, Marc. Jothan?

JOTHAN FRAKES: Yeah. So line 47 and the sentence that it continues into line 48, this makes a statement that says, "Threat actors register large portfolios." Threat actors also individually register domains. I don't know if we want to condition this to say for scenarios where threat actors register large portfolios or register portfolios. Thank you.

PAUL MCGRADY: Thanks, Jothan. So what's the textual change you're looking for?

JOTHAN FRAKES: Yeah. Let me put a suggestion in, because I think it would modify the sentence slightly.

PAUL MCGRADY: Oh. Are you putting that into the document? Or... Because if you can tell us what the textual change is, staff can grab the idea.

JOTHAN FRAKES: Apologies. I'm navigating, hopping between Zoom and the document. I'm the elephant in the document.

PAUL MCGRADY: The threat actors.

JOTHAN FRAKES: So that would be the change I'd suggest. Threat actors might register portfolios consisting of multiple malicious domains to enable them to launch coordinated or multiple separate phishing or malware campaigns at scale.

PAUL MCGRADY: Thank you, Jothan.

JOTHAN FRAKES: Otherwise, we're assuming threat actors always do this. Yeah.

PAUL MCGRADY: Okay.

JULIE BISLAND: Paul, we're having trouble hearing you.

PAUL MCGRADY: Yeah. Marc, any concerns with Jothan's tweak to your tweak?

MARC TRACHTENBERG: No, I just said in the chat, fine.

PAUL MCGRADY: Okay. All right. Well, we've heard several in the chat, I think, say these are good changes. We've had some tweak the changes, and we've heard from Reg that she does not like the change. Any other pushback on this change or these changes? Feodora.

FEODORA HAMZA: Hi, this is Feodora. I don't have any pushback, sorry. We just wanted to note that this part of the initial report is not related to any recommendation, rationale, or implementation guidance, so it's not binding, just for clarification. And most of the text has been taken from the charter itself. So, just to note when the working group works on it and decides on wording to have that in mind. We just wanted to clarify.

PAUL MCGRADY: Thanks, Feodora. Yep. No, I appreciate that. On the other hand, the charter is what Council spoke. This report is what we speak. So if we want changes, we make changes. But it is good background. All right. Let's move on to the next page, see what's there. All right. On the next page. Looks like Martina had a suggestion. She's not here, so maybe we can hear from someone else from the GAC. Oh, Martina, you are here. I thought they said you weren't.

MARTINA BARBERO: No, there was a misunderstanding with Gabe around my dates. I'm here, but actually that was a point from Brian, so I think I just plus one on Brian's suggestion.

BRIAN CIMBOLIC: Yeah. Hi, Paul. Hi, Martina. Happy to jump in, Paul.

PAUL MCGRADY: Oh, go ahead.

BRIAN CIMBOLIC: Yeah. So thank you, and good morning, good afternoon, good evening, everyone. This is a change that echoes another change I suggested in the document starting at line 300. We don't need to jump there, but just you're going to hear this twice. This gets to the notion of the fact that we want to be careful in not writing the policy in such a way that it is necessarily restrictive. So if a registrar wanted to conduct a robust associated domain check, that they would be prohibited from doing so. I think that the notion is more that it's a restriction as far as how ICANN can enforce it. So ICANN can't require a registrar to go and violate applicable data laws.

So really the substance is there, the protection is all there, but it's a reframing just to ensure that in interpreting the policy, these protections should be viewed in the lens of ICANN cannot require a registrar to do any of these things. It's sort of more clear in the change to 300. What we don't want to do is end up creating a ceiling in which a registrar is sort of discouraged from worrying about going too far in conducting the associated domain check, not from a legal perspective, not from a data perspective, but from an ICANN compliance perspective. So I tried to come up with some language to that effect.

PAUL MCGRADY: Okay. So the comments on this document were positive. The comments to your suggested changes within the document were positive. Let's do a verbal queue on this. Farzi, go ahead.

FARZANEH BADII: Well, hello again. So basically, we were very happy with this language because it does kind of provide some kind of guideline on how it should be interpreted. So if it can be moved to implementation guideline, that's great. And also, we really like that it says that. We had a conversation about this on the mailing list, and also with Becky during our last in-person meeting. But so we very much like to keep this language that Brian has deleted. So wherever you can put it that just addresses both concerns. And also, I don't personally agree with the argument that ICANN cannot enforce privacy and data protection standards, but that's another, a larger debate. So I don't agree with Brian's argument on this. If ICANN is obligating the registrars to do something such as associated domain check, they can also obligate them to do it in a privacy-respecting manner. But with this language that has been deleted, we would like to have it elsewhere if possible. It's important for us. Thank you.

PAUL MCGRADY: Thanks, Farzi. I do know we've built a lot of safeguards in talking about proportionality and other things. I'm trying to understand the ask. Is there something in the deleted text that you think is not addressed someplace else in the report?

FARZANEH BADII: Yes. So I think that this minimization, including respect to proportionality, evidentiary standard safeguards, operational consideration, and efforts to minimize false positives and collateral impacts on legitimate registrants, I think these are really important points. And if we can put them somewhere, like in the implementation guidelines, that would be great. So you can delete it from here, but put it somewhere else.

PAUL MCGRADY: Okay. So Farzi, I'm going to ask you to do that homework and tell us where you would like to see it moved to.

FARZANEH BADII: I will do that.

PAUL MCGRADY: Okay. Thank you. All right. Any other questions on Brian's approach here? Okay. I think that takes us now to a Trachtenberg item. And if a different course is chosen by. Marc, do you want to speak to this? And I'd especially like to hear from you about the reason for this sentence, because this is already part of the IRT's obligations. They have to provide a rationale, but tell us why you would like to see it again here.

MARC TRACHTENBERG: I just thought it was important to emphasize, but if it's completely redundant, then we can remove it. We have redundancies in a lot of other places to emphasize certain points, but if it's completely superfluous, then it can come out.

PAUL MCGRADY: Yeah. It's my understanding, and staff can correct me if I'm wrong, that whenever an IRT deviates from implementation guidance, then they have to provide a rationale. So to me, it's redundant, but anybody want to advocate for keeping it? Okay. All right. Let's back up. Farzi, go ahead.

FARZANEH BADII: I just want to say that I think that Marc's comment here kind of points to another issue, which we should be clear to the WG, the working groups in general, and how IRT works, so that they know that their concerns are addressed and IRT won't deviate from what is being suggested by the group just on its own.

PAUL MCGRADY: So Farzi, is that an advocacy for keeping Marc's language?

FARZANEH BADII: No. But I think that it generally demonstrates that we need to be clear about IRT process more.

PAUL MCGRADY: Got it. So more of a macro issue that it would be helpful for working groups to understand how IRTs function. Okay. All right. Next up, is it Martina?

MARTINA BARBERO: I'm afraid not, Paul. I think this is a suggestion from the NCSG. I don't know why you keep saying my name.

PAUL MCGRADY: Oh, I'm sorry.

MARTINA BARBERO: No worries, no worries.

PAUL MCGRADY: Well, I'm just reading down the list. Maybe I'm not seeing... I wonder. Oh, I see. These are follow on. I'm confusing myself with follow-on comments. Perfect. Okay. This is unfortunately old man syndrome. It's hard to know which comment goes which. But Martina, you're my favorite person to call on when it's not your turn, so I think that's important to keep in mind. It's out of favoritism. All right. Michaela, this is actually yours. Please go ahead.

MICHAELA NAKAYAMA SHAPIRO: Thanks, Paul. I know it's confusing when the comments are kind of all spread across the page. So thank you. Michaela, for the record. So this was a recommendation from the non-commercial side, as we were

concerned that, yes, we've talked a lot about how the scope of the charter makes it so that compromised domains are out of scope, but we were concerned that that wasn't quite a step that made sure that we actually did some kind of assessment to show that a registrar has actually assessed whether it's a compromised or abusive domain prior to triggering the ADC. And so we had put in some language, and then after that, we were able to confer with the registrars on this. And so we've actually proposed new language again here. And so the final language that we really want to put forward for consideration is this bit about, that I bolded just to try to make it clear, "And the registrar has reasonable belief that the Registered Name is not a compromised domain." And we want to hear what folks think about this. I don't know, Martina, if your hand is about that particular one or because you want to come in next, but maybe I'll stop there and allow for folks to ask questions.

PAUL MCGRADY: Thanks, Michaela. Martina, go ahead.

MARTINA BARBERO: Thank you very much, Marc, and this time it's actually me wanting to comment. But Michaela, thank you very much for the explanation. We understand the spirit of this suggestion. We're not convinced. We feel it's a bit redundant in that it's already quite clear that this policy does not apply to compromised domains. And we feel also it hikes the thresholds for the registrars who will have to also demonstrate to ICANN compliance the evidence for a reasonable belief that the Registered

Name is not a compromised domain. So, all in all, we feel it's unnecessary and also a bit late in the game for this recommendation that we have been discussing for a long time. But keen to hear what others think. We also saw the registries reacting to that. So I'm keen to hear from others.

PAUL MCGRADY: Thanks, Martina. Marc?

MARC TRACHTENBERG: Yeah, I agree with Martina's comments, and I'm not sure how the registrar is going to demonstrate this. And comments that were made earlier were that the registrar shouldn't have to read the mind or read the tea leaves. And I think here, this change again makes them read the tea leaves and take another step of trying to go beyond it and figure out, in every case, whether it's compromised or not. And then they're going to have to somehow demonstrate this to compliance, which I think will also be challenging and add additional record-keeping requirements, which I understand is not wanted.

PAUL MCGRADY: Thanks, Marc. Farzi, go ahead.

FARZANEH BADII: From the start of this working group, we have warned about false positives, and also we have presented a case that a false positive happened. And then one of the things that this group kept telling us was

that, oh, this only applies to compromised domains. So we compromised on the language for threshold and other things, despite the fact that we don't agree that excluding compromised domains is enough safeguard. And now not obligating the registrar to demonstrate how they are actually—and it's a really easy thing. They do it all the time. So how they are not doing ADC on compromised domains, then that thing that we've been discussing and the safeguard that we've been talking about is kind of redundant here. Of course, they should demonstrate. And demonstrate that it's not like, what are their methods not to entangle a compromised domain? Because we are worried about surveillance that can happen on innocent people. Thank you.

PAUL MCGRADY: Thanks, Farzi. Before you go, I guess I'm a little confused then about whose comment this is, because I thought this was an NCSG change, but you seem to be speaking against it. So help me understand.

FARZANEH BADII: No. NCSG change says that registrar has reasonable belief that the Registered Name is not a compromised domain. And we are talking about that.

PAUL MCGRADY: Got it. Okay. So you're not against the change, you're for the change.

FARZANEH BADII: No. Of course, I'm against the counterarguments that is being presented by Martina and Marc.

PAUL MCGRADY: Got it. Okay. Terrific. Thank you. That's helpful. Christabel.

CHRISTABEL MEBAGHANDU: Thank you very much, Paul. Good day, everyone. This is Christabel Mebaghandu for the record. So I just want to echo Michaela's points on excluding or including language that's currently sitting, I think, in the implementation guidance, just moving it up to the recommendation itself. I believe that if we don't spell that out in the recommendation itself, I think that the policy would ultimately risk subjecting every single abusive domain, including potentially compromised domains, to portfolio-wide checks, and afterwards potentially realize, oh, that this 1% or 2% of reported abusive domains are actually compromised after the check. And what we have simply done in that scenario is subject compromised domains to unwarranted, absolutely unwarranted portfolio-wide checks. So what I would like to know from our colleagues who would object to this is how, based on the creed of this working group to protect compromised domains from these checks, how do we aim to protect them given the definition of the trigger and the operation of the trigger itself and everything in between, if we are not spelling out that we have to exclude these compromised domains before actually triggering a check?

PAUL MCGRADY: Thanks, Christabel. All right, Michaela, you're back.

MICHAELA NAKAYAMA SHAPIRO: Thanks so much, Paul. Yes, kind of piggybacking a bit on Farzaneh and Christabel's comments, which I hope I can also try to address some of the pushback we've gotten so far. So the idea is not to make this an extra step per se. We're not trying to make this overly onerous. When we spoke with the registrars, the idea was that actually a number of registrars already take this step, to at least do some kind of initial assessment prior to triggering the ADC. And that's fantastic, and we want to see that continue. And the idea is to make just that step the requirement here, so that you just showcase that you have at least taken, based on the evidence you have at hand at that stage, that you've taken the step to try to determine whether this is a compromised or abusive domain, not to be penalized if you get that assessment incorrect. So to Marc's point earlier, this isn't about the accuracy of the assessment, and it's not an extra step for most of the registrars that are already doing the right thing, as we've been talking about a lot as the NCSG. What we really want is that this be operationalized, standardized, and a requirement for registrars beyond just the ones who are already doing the right way or taking this step already. So I hope that that is helpful. Yes, so we do not want it to be required on that, and at the same time, our concern is that the way that the policy is written at the moment, yes, it does not extend to compromised domains, but it doesn't say that you actually have to determine how. There's no step for the how of determining whether it's a compromised or malicious domain. So our hope is that here it can just be one small addition for the registrars that aren't doing it, and really no change for the registrars that

are already doing it. And the proof to prove to compliance would be very much a, "I took this step based on what I did, and here's what I did." And that is already going to be part of the ADC process in terms of proving compliance. So I hope that's helpful, but curious to hear what others will say. Thanks.

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

GABRIEL ANDREWS: Hi, it's Gabriel Andrews for the record. So I have two concerns with this language. One is with regards to the legal threshold, at least in the term reasonable belief means something in the U.S. legal context that I'll get into in a second, and then the second is operational. So addressing the first. A reasonable belief is a legal standard that, at least in my line of work as law enforcement, that's what you have to hit in order to do things like execute a search warrant on someone's home or arrest someone. It typically means that I've compiled a 20 to 30-page affidavit of facts and swear to those facts before a judge in order to convince a judge that there's reasonable belief. This is what it means in the legal context to my experience, and it is a very high standard to suggest that that's the kind of threshold that you're expecting a registrar to meet prior to being able to do an ADC. That seems like quite a laborious stretch to do something that is rather a preliminary investigative step that would enable you to collect the facts necessary to reach that standard. So I think it's cart before the horse as written.

Secondly, now returning to the operational concern. Consider the scenario where a bad guy has compromised a customer account at a registrar. There are existing domains in that registrar's portfolio. The bad guy uses that compromised access to both register maliciously new domains using that compromised account, as well as use some of the existing domains for harm. Now, if there is a report of abuse for that scenario to occur, does that mean that this means the registrar can't look at the preexisting domains to see if they're being used for harm so they can tell their customer? It seems to be a prohibition against it. I have concerns with that. That seems to tie the hands of a registrar that would want to protect their customers. I don't think this takes into consideration operational realities. So those are my concerns at the start. I think I've said enough. Over.

PAUL MCGRADY: Thanks, Gabe. All right, Reg.

REG LEVY: Thanks. The Registrar Stakeholder Group appreciates the NCSG's concerns and their adjustment to this language and supports it.

PAUL MCGRADY: All right. Jothan.

JOTHAN FRAKES: I threw my hand up because there was a suggestion to move some of this up from implementation guidance to recommendation, and I

wanted to just state that we have found a balance with this with respect to how it would manifest within compliance and in finding a reasonable ability to meet this. One of the consequences of moving it from implementation guidance, or moving anything now from implementation guidance into recommendations, is that that is the more enforceable area. And I think we would have to then rework the wording if we were to make such a large move at this point. So I wanted to oppose it just for that purpose, that we've spent some time to get to a balance here. Thank you.

PAUL MCGRADY: Thanks, Jothan. It's interesting conversation. I'm going to pause here for a minute, and then we'll go to Michaela again, but lots of chat in the chat as well on this. Yeah. One is collecting facts, right? To reasonably demonstrate that something is not a compromised domain. And the other one is this reasonable belief standard. The registrars say they're okay with it, but maybe I just think a little bit too lawyerly because my concern, of course, is that ICANN compliance just says, "Well, we disagree with you. It wasn't reasonable." Right? And then you're in breach. And then you go through that merry-go-round two or three times, and the registrar's in hot water. And especially if there's a desire to not create a bunch of new records. But ultimately, this is a representative model, so my concern for the registrars, if they don't have the concern, then it's mind your own business time as chair. But I heard what Gabe had to say about reasonable belief, and I think that that's something that's a big deal. Let's talk about... Well, let's not. Michaela, why don't you jump in?

MICHAELA NAKAYAMA SHAPIRO: Thanks. I'll try to keep it short and sweet. And I completely appreciate Gabe. I don't work in law enforcement, nor am I a U.S.-based lawyer or a lawyer, period. But my understanding is, I think this is quite different in terms of the context in which it'll be applied and my understanding. And we do have lawyers from the registrar side who are saying that this isn't overly onerous, and I'd like to have faith in their understanding of how that standard is applied here. In terms of putting the cart before the horse, I think to an extent, this charter is almost asking us to have to do that. And I'll clarify what I mean by this, which is I think we're concerned about having too much faith in the statement of this requirement does not extend to compromised domains without having discussed any ability to actually distinguish between compromised and malicious domains. So really, my question then is, how do we then actually put this in practice? We say that compromised domains are out of scope, and that's great, but I still have some concerns about how do we actually rule that out, and at what stage does that take place? So if it's not at this stage, then at what stage are we then saying that we're actually implementing this distinction? So that's my concern. But I do think that actually is within the group's remit because the charter has asked us very clearly to exclude domains that have been compromised when it comes to this obligation. So understand that the obligation to do so is different than requirement to do so. But again, I want to understand from the group at what stage are we then saying that we are actually doing this distinction and how? Thanks.

PAUL MCGRADY: Yeah. Thanks, Michaela. So before you go, can you react to Jothan's concern that, as you stated, this is the how, right? And usually the how ends up in implementation guidance. Can you address Jothan's concerns that this is implementation guidance?

MICHAELA NAKAYAMA SHAPIRO: My understanding is this is the requirement to do the how. This is operationalizing the how. Right? This is an action that also gets at the how, if I haven't abstracted that completely. But that's if I understood Jothan's concern. And again, I think we can also discuss more, but I wanted to really stick to the points that seem to be really getting at the heart of this concern. And I also want to make sure that Martina and Chris get their time, and Farzi, if she wants to come in on that part or wants to respond later on. But yeah. I'll pass it back to Paul here for the queue.

PAUL MCGRADY: Thank you. Farzi, welcome back.

FARZANEH BADII: Thank you, Paul. I know you're delighted to have me on this call. So, okay. So Gabriel said something. It seems like he has the impression that through this policy, we are obligating the registrar to also do ADC on compromised domains. That is not true, and that is not within the scope. And every time we talked about a trigger threshold, they said, and we talked about taking innocent domain name registrants, like false positives and stuff like that. Every time, there was the argument that we

are not talking about compromised domains. Okay. So if the group has this impression that compromised domains is in the scope, let's go back to the drawing board. If it is out of scope, then we need to be clear on a definition of compromised domain and a malicious domain and say that explicitly in our policy. That by malicious registered domain, we mean this. By compromised domain, we mean that. And also, we can get help from our SSAC friends. But all in all, it sounds clear to me, and I said this from the beginning. Unfortunately, the line between maliciously registered and compromised domains is very blurry, and innocent registrants will get caught in this. But anyway, we are not asking the registrars to do much more than what they are doing already because they already say that they do this on maliciously registered domains. So let's just have a definition or let's put it in the implementation guidelines. But if you say that compromised domain are out of scope, they should be out of scope and it should be demonstrated that they were not caught up in this kind of ADC. Thank you.

PAUL MCGRADY: Thank you. All right. We have Martina, and then two others, and we are going to have to get moving if we're going to get through this. We don't have that much time left, and we want to make sure we get the full reading. But that is not to rush Martina, Chris, or Theo. Take your time. But I'm just telegraphing we're going to move on from this here in just a little bit. Martina.

MARTINA BARBERO: Thank you, Paul. And I'll be very brief. I think for the GAC, it is quite a surprise that now we're reopening the text of recommendations as such. As Jothan said, this was a compromise as well, and a delicate balance that we found with this recommendation. Personally, I think for my constituency, we'll have to bring it back to the GAC, but it's something very difficult for us to accept as is. And especially, I'm not sure whether we want to start reopening all the recommendation at this stage. But we will bring it back and we hopefully can discuss it more in the context next week.

PAUL MCGRADY: Thanks, Martina. Yeah, no, I want to be clear that the goal of this review is not to reopen language that's been stable for a long time. Well, I don't want to jump to the end. Okay, I won't jump to the end. Chris, go ahead.

CHRIS DISSPAIN: Thanks, Paul. I might jump to the end on your behalf, or rather not on your behalf, instead of you. So starting with my lawyer's hat firmly screwed on to my head, I want to echo what Gabe said. Reasonable belief is a really challenging term. In many jurisdictions, it has a very specific meaning. I'm slightly perplexed that there appears to be, and I may have misunderstood, but if the registrars think that reasonable belief is a lesser requirement than reasonably demonstrate, that is not the way that I would interpret it. I would argue that reasonable belief means a very strong requirement, that they will have to go through a process to determine that they reasonably believe that this domain is not a compromised domain. So I'm not really clear why that would be

more acceptable to registrars than reasonably demonstrate, which I don't think has anything like the same, if indeed any, legal precedent as a term, and can be interpreted in a much sort of simpler way. And I also just wanted to briefly echo Martina's point about reopening because this is quite a substantive suggested change. And we really are at a point, I thought, where we'd kind of gone beyond this, and we shouldn't really be discussing something quite as substantive as this. Thanks, Paul.

PAUL MCGRADY: Thanks, Chris. Theo, go ahead.

THEO GEURTS: Yeah, thanks. This is Theo, for the record. So I don't mind the language, but when we are talking about what a case is, it all starts with the report. And if you look at the reporting nowadays, especially from the commercial outfits, and 99% of the reports are from commercial outfits. The majority, I would say, with an exception here and there, are very substantive, and you know from the get-go what you're dealing with. Is it the compromised domain name? Is it the malicious domain name? It really starts there. So I don't have any issues with the language as such, because most of the reports are laid out in such a fashion that any registrar with a brain cell here and there knows exactly what they're dealing with. Thanks.

PAUL MCGRADY: Thanks, Theo. Michaela, we'll give you one more hearing on this, and then we do need to move on.

MICHAELA NAKAYAMA SHAPIRO: Appreciate it, Paul. Thank you again for handing me back the mic. Just wanted to reiterate the conversation in the chat here. We are not trying to upend work or substantively change this section. We actually understood this to be relatively minor, and that's why we came to this compromise language with the registrars. We're frankly quite surprised that this has kicked off a bit of a firestorm. So very happy to come back to this. I understand we've devoted a lot of time to today. Very happy also to chat offline. Again, this is not trying to upend or open a new conversation. We understood this as after having done a holistic review of the text, this is a gap that stood out to us, and we wanted to come back to it now that we have done a holistic review of the entirety of the draft text. Thanks.

PAUL MCGRADY: Thanks, Michaela. All right, jumping to the end, which is this is a proposed change to fairly stable recommendation language. Those kinds of changes, if they are by widespread applause, generally make it in, but we've heard strong opinions on both sides of this. We're not getting traction to reopen something. This is not to say that people can't work offline. Knock yourselves out, for sure. And if everybody can get there, then we can bring it back up. But as it is now, I didn't hear the level of support necessary for a late in the game change. So things to think about if you are going to try to work it out offline is, do you really need to mess with the language of a recommendation at this point, or could this be in implementation guidance? That was Jothan's suggestion. All

those things. So feel free to keep working on it, but we don't have the support for the change at this point.

All right. We're moving on to the next comment, which is swapping out the word active for occurring. It's a comment by Rod. I don't know if, Rod, you want to explain why, or if it's obvious enough to everybody for the change.

ROD RASMUSSEN: Hopefully obvious. I'll explain the change right afterwards, just a term of art confusion for clarification. Thanks.

PAUL MCGRADY: Got you. Thanks, Rod. Any issues with changing active to occurring? Any hands? Okay, no hands on that, so we'll take that one on. The next one is pertaining to the same abuse scheme and/or abuse vector. This is, again, well-settled language, but Marc would like to address it. Marc, go ahead. Oh, Jothan, go ahead.

JOTHAN FRAKES: Go ahead and take Marc first.

PAUL MCGRADY: Okay. Marc?

MARC TRACHTENBERG: Sure. This is similar to my kind of comments in the preamble. So it says abuse report submitted to a registrar should include sufficient information and evidence to support the reported allegations of DNS Abuse. That's right. But when you say pertaining to the same abuse scheme and/or abusive actor, if there's just one domain name that's being reported, how could the person have to include in the report that the abuse relates to something else common? That's the entire purpose of the ADC, is to identify other related domain names when the reporter is only reporting one domain name. And so this kind of expands the requirements in 3.18 in the RAA. All that should be required in the abuse report is that—

PAUL MCGRADY: Yeah. So Marc, this is language related to what a reporter needs to put in here. Abuse reports submitted to a registrar should include sufficient information and evidence to support the reported allegation of DNS Abuse.

MARC TRACHTENBERG: Exactly. It's what the reporter is reporting. And so if the reporter is reporting one domain name, how can they be required to put in evidence of a common scheme or abuse with other domain names when they're only reporting the one domain name? This is the purpose of the ADC. That when you report one domain name, the registrars check to see if there are other related domain names that are also being used for abuse. So this is way putting the cart before the horse and

defeats the purpose of the ADC. You can't require the reporter to have to do all the work and report the ADC.

PAUL MCGRADY: So Marc, instead of striking this, so I guess I'm trying to understand why the IPC would not want a reporter to know that they should, if they have the evidence of abusive scheme or abusive actor doing more than one thing, why that wouldn't want to be in there. Are we just missing some language between these two concepts where we say something like, "Evidence to support the reported allegation of DNS Abuse, comma, and if relevant, evidence pertaining to the same abusive scheme and/or abusive actor"? Or do you just want that thrown out?

MARC TRACHTENBERG: It should be thrown out because all that's required is that they submit evidence of DNS Abuse for one domain name. That's what the trigger is. Why should they have to include evidence of other domain names? If they have that, of course they're going to include it, but I don't know why we need that in the guidance. If the reporter knows of five domain names being used for a common purpose, they're going to report all five, not just one. Right now, unfortunately, in a lot of registrars, you can only report one domain name per report. And so actually, the way the registrars have it set up in a lot of cases for abuse reporting, you can't even do this. You can't even include the other domain names. You can only include the one. But that aside, taking that out, again, the trigger is one domain name being used for DNS Abuse. That's all. We don't need any guidance saying that the reporter should or has to include evidence

of any sort of common scheme because, again, that is the purpose of the ADC.

PAUL MCGRADY: Yeah. Okay, thanks, Marc. I think we're sort of looking at this in isolation when it wasn't created in isolation. It was created to deal with the situation where a domain name is no longer observable doing the abusive thing, because the abuse is intermittent. And if there's an intermittency claim, then the reporter needs to provide that information, rather than requiring the registrar to go fishing for it. But you are talking purely about trigger as opposed to intermittency. So, again, I'm going to keep asking you if you really want this out. Jothan?

JOTHAN FRAKES: Yeah. So this particular one, we do get reports for multiple domains. There are registrars that do accept those, and people find their way to reporting multiple domains. But setting that aside, we had carefully negotiated this text to deal with reducing friendly fire and the situation where the domain has changed hands and is clearly not used in the same way and is not owned by the same party or used in the same campaign. This could be the case, and unfortunately, I think, in the process of getting the evidence or whatever occurs, there are some reporters where the report might trail months, and in some cases, years after the actual activity at hand. And the domain name may have been deleted and then re-registered by another party. The domain name may have been seized by the registrar and sold to another healthier party who's using it in healthy use. So this was to make sure that a report of

prior malfeasance is not applied to a new party, and that was why that text was there that is being stricken out. This gives the registrar room in a situation where clearly it's not the same party to not take friendly fire action or harm a healthy registrant. And that was why we had negotiated this text. Thank you.

PAUL MCGRADY: Thanks, Jothan. Marc.

MARC TRACHTENBERG: So I'm okay with adding "and where relevant," but maybe the better way to do it is to say abuse reports involving domain names where the abuse is intermittent should include sufficient information and evidence to support the reported allegations of DNS Abuse, and we can put the rest in. I think that maybe clarifies it, because otherwise it's not so clear. It seems like it's referring to all abuse reports, but it seems to me, based on this discussion, that it's really tied to the previous sentence, which I think is not so clear in the current text. And so if that sentence is only supposed to apply to reports of intermittent abuse, let's just clarify that in a sentence.

PAUL MCGRADY: Well, I think we clarify that by putting in "and where relevant" and putting back in the proposed text that was struck.

MARC TRACHTENBERG: And so, like I said, I'm okay with that language.

PAUL MCGRADY: Yeah. Okay. Yeah, let's not rework it too much that we lose the theme. Anybody opposed to "and where relevant" to bridge the two concepts in that sentence, raise your hand and say, "No, thank you," to "and where relevant." Jothan, go ahead.

JOTHAN FRAKES: And so we would unstrike the struck?

PAUL MCGRADY: Correct.

JOTHAN FRAKES: No, I would be good with that. Yeah. Thank you.

PAUL MCGRADY: Perfect. Farzi.

FARZANEH BADII: Hi. We are generally okay with "where relevant." So, how is this going to read? Support the reported allegation of DNS Abuse and where relevant what?

PAUL MCGRADY: And where relevant, sufficient information and evidence to, uh...

FARZANEH BADII: The same abuse—

PAUL MCGRADY: Great question, yeah. Maybe staff can help us wordsmith that. But essentially, it's the same standard. Sufficient information and evidence to support claim that more than one domain name are involved or pertain to the same abuse scheme and/or abusive actor. We're going to have to figure that out, Farzi, but we will. We'll come back to you in the next reading. But that's the concept.

FARZANEH BADII: So I just want to flag something.

PAUL MCGRADY: Yes.

FARZANEH BADII: If you have abusive actor there, we are not going to agree with having abusive actor there. You can talk about the scheme and other things, but we think that it will go back to the registrant, and we don't want the term abusive actor. Thank you.

PAUL MCGRADY: Okay, Farzi. Unfortunately, that phrase has been in here for weeks and weeks. So—

FARZANEH BADII: No. No, Paul. Abusive actor was added by Gabriel last week. It was a suggestion by him, and it was actually the change is great. We agree with the change. We don't want the identification of domain name registrant here. So the change is good not to have the domain name registrant, but what was added was the same abuse scheme and/or abusive actor. We are just saying that we don't want abusive actor there. Thank you.

PAUL MCGRADY: Okay. Let's hear a sub-queue on that. All right, Jothan, go ahead.

JOTHAN FRAKES: Yeah. It's still struck out in the document. I don't know if Marc, if you can undelete it. But basically, it sounds like the issue is where it's the same party. And one of the things that observed is that a malicious registrant might change the contact information or alter it after a report and make modifications. And so what I was asking for was to try and guard an innocent new Registered Name Holder from being swept in with the rest of the debris. And the way we split hairs on this was to make sure that, yes, you can prove it's not the same party through some means. So abusive actor would be where there's other indications that the reported party, even though the domain name might state a different registrant name or something of that effect, that there would not be a situation where that party could slip through the cracks here. We want to find the Goldilocks, not too hot, not too cold kind of wording here,

and that was where we had arrived. Now, I see Gabe's hand up, and he's far wiser than I am at this, so I will shut up and let him talk. Thank you.

PAUL MCGRADY: Thanks, Jothan. Gabriel?

GABRIEL ANDREWS: Yeah. So plus one everything Jothan said, but Farzi, can you explain why don't you want a registrar to be able to associate domain checks for domains being maliciously registered by the same abusive actor? That seemed to be exactly why we want these to occur. So why not?

FARZANEH BADII: Can you remind us, Gabriel, why you suggested to make this change to remove a domain name registrant? And I think Christabel has a good answer for you. But if you can remind us why you made this change from a domain name registrant to abuse scheme or abusive actor.

GABRIEL ANDREWS: For the reasons Jothan just explained, essentially, that we aren't trying to use the registrant information field that often is changed by the bad guys, nor are we trying to suggest that is the key piece of information that we care about. What we care about is, are there maliciously registered domains being used either within the same abusive scheme as we talked about, or by the same maliciously registering bad criminal actor who might be doing more than one scheme at a time. And that's the reason why I'm a little bit concerned about limiting only to single

scheme, because that means if this guy is doing multiple things, let's say he's doing business email compromise schemes against a financial industry while simultaneously sending phishing messages to biotech firms. If it is demonstrable that he's doing all of this at the same time, and it's the same person, and there's enough evidence to point that these are all malicious registrations, I don't see why we'd want to handcuff ourselves to only the same scheme here. But maybe you have a reason for that, and so that's why I'm asking for clarification.

FARZANEH BADII: So the reason—

PAUL MCGRADY: Sorry, Farzi, I have to maintain control of the queue.

FARZANEH BADII: Go ahead. Yes.

PAUL MCGRADY: I just can't turn over the call. Sorry. All right. Let's hear from Christabel, and then from Marc. And Farzi, if you want to get in the queue, we'll cut it off there. I am not hearing widespread support for striking abusive actor. So, and again, this is fairly stable language, so we're not meant to re-litigate all of this. And we're on page five of 24. So unfortunately, I feel like we're doing what we're not supposed to do, which is take the fourth bite at every apple we didn't get. Christabel, go ahead.

CHRISTABEL MEBAGHANDU: Thank you. Christabel Mebaghandu for the record. So aside the very rich exchange that was going on between Farzaneh and Gabriel, I just wanted to quickly chip in that if we are looking at individual registrants, in the case of abusive domains, without explicitly providing those safeguards against, again, what I was speaking about earlier, which are compromised domains, I feel that we might not exactly be doing such a great job. I think that it would be great to keep things narrowly scoped around an abuse scheme or an abusive domain. This might just be one of those elements that might have broader implications than in just one section of one certain implementation guidance. I think that we should just give it some extra thought. That's just what I wanted to chip in. Thank you.

PAUL MCGRADY: Thank you, Christabel. Marc?

MARC TRACHTENBERG: I would just point out that this doesn't really have anything to do with individual registrants. This is not what the registrar is looking at. This is not part of the ADC. This is what the reporter is reporting in their DNS Abuse report. And in 99.99% of the cases, they're not going to know who the registrant is because that's hidden either behind a proxy or due to the RDP. So all this is, is again, tied to the previous language talking about intermittent abuse, in accordance with what Jothan was saying, trying to ensure that there's not overreach here. And so this has no risk to individual registrants or is not related to them in any way. All this is, is

what is in the report from the abuse reporter, if they have some evidence that the intermittent abuse is related to a common scheme or the same actor, which is, at this point, an anonymous actor who they don't know who it is. So I just don't see that there's any risk here from threat actor or abusive actor.

PAUL MCGRADY: Thanks, Marc. Yes, this is about what the reporter will be reporting. And it's specifically designed, I thought, to make it not the registrar's problem to go in and develop new reports and information about the behaviors of a particular actor to see if they are an abusive actor, a repeat abusive actor. But rather, if the complainer has information, they should feed that into the system. So again, I think we've kind of gone a little bit outside of what the sentence actually says here. Okay. Great. We have to move on. We have only 10 minutes left and, in theory, 21 pages to cover. We're not going to do that, obviously. Let's see here. Our next comment is a Trachtenberg comment. Quite a bit of text here. Marc, you want to go ahead?

MARC TRACHTENBERG: Yeah, I'm just reading my comment. Right. So here, I think there's some conflation on what's being talked about in that compromised domains are separate from where the domain name itself is not compromised, and the domain is generally being used for non-abusive purposes, but there is DNS Abuse happening through the domain. And so this is what I'm trying to clear up here.

PAUL MCGRADY: Okay. Brian, please react to this.

BRIAN CIMBOLIC: Yeah, no, actually, thanks, Marc. It's more just a question. If it's okay to ask a question, Marc, could you give an example of what's the fact pattern you're trying to protect against?

PAUL MCGRADY: Yeah, Marc, please go ahead.

MARC TRACHTENBERG: So I think the fact pattern here is, in some cases, the bad actors will register domain names and only include abuse in a small part of the domain name. Or they'll create a whole website, they'll have a lot of stuff that looks legitimate, and only certain parts are used for abuse. And so does that fall into the category of the domain name is registered for the sole purpose of conducting DNS Abuse? That's kind of the case that we're trying to address, because they try to hide their abuse.

PAUL MCGRADY: Brian, do you have a reaction to that?

BRIAN CIMBOLIC: It's just a thought, and I get what you're getting at, Marc, and I'm sympathetic, but I think that it becomes really hard really quickly to implement that. So if you look at, for example, a subdomain provider, it might be that it's a heavily exploited service, but there might be a solid

mixture of DNS Abuse and non-DNS Abuse. So I think it becomes hard to implement pretty quickly unless you can find a way to neatly tie a very specific fact pattern in a bow. I think that becomes pretty tough.

MARC TRACHTENBERG: So in the scenario I discussed where there's a lot of legitimate looking content on the domain name and there's only certain URLs on the domain which the bad actor is using for abuse and directing people to those URLs, does that qualify for being used for the sole purpose of conducting DNS Abuse?

PAUL MCGRADY: Okay. Marc, I understand the concern you're raising, and you're seeking granularity on this. But up until today, it's been a binary, right? Either it's a compromised domain name or it's not. If it's compromised, then it's out of scope. If it's an abusive domain name, then it's in scope. And so if you have a domain name that is registered by an innocent party that's using the domain name and for good reasons, but there's some small part, as you say, that is compromised, and being exploited by a third party malicious actor, then that's compromised. So I'm—

MARC TRACHTENBERG: Right. I'm not talking about compromised domains. Those are out. I agree. So that's the kind of clarification I tried to make, where if the domain name is used for non-abusive purposes, like if you have a social media site and one of the users is engaging in DNS Abuse, that wouldn't be included in here. But what I'm trying to clarify is in the situation

where it is a bad actor. They've registered the domain name for DNS Abuse purposes, but a lot of the content appears to be legitimate on the domain name. It's not, it's just a cover. But there's only DNS Abuse occurring in parts of the domain name because the bad actor is trying to obfuscate what it's doing. In that situation, I'm asking, does that qualify as a domain name that's being used solely for DNS Abuse if the rest of it's not, to obfuscate that behavior? Because that is what increasingly happens. The bad actors know that we are onto them, that we monitor, and so they hide it in part of the domain name.

PAUL MCGRADY: So Marc, how do you calculate primary purpose? I understand solely. Solely is a zero or a one. How is a registrar—

MARC TRACHTENBERG: I don't know the answer to that question. A lot of judgment calls are being required to be made in this policy.

PAUL MCGRADY: Okay. So from my point of view, that's a completely new calculus that we're trying to put onto the registrars, and we are late in the game for that. Chris, go ahead.

CHRIS DISSPAIN: Thanks, Paul. Just to say, irrespective of whether it's a good idea or it isn't a good idea, it's not rationale. It's not an explanation. It is a whole new thing, so it doesn't belong in rationale anyway.

PAUL MCGRADY: Yeah. Right, it's not a rationale. It might be implementation guidance.

MARC TRACHTENBERG: Okay. I accept that.

PAUL MCGRADY: Yeah. Okay. All right. I think the takeaway here is, Marc, if you want to rework this, or anybody wants to work with Marc to rework this, again, everybody's allowed to talk, more words the better, offline. And if there's something here that you can get a generalized agreement from most everybody around, we can figure out where to put something like this. But from my point of view, I don't know how to calculate primary purpose, and we've said from the beginning that compromised domains were out of scope and we've had the word solely, I don't know how many weeks we've had the word solely. So it's a fairly significant last-minute change. So unless we have some widespread acclamation for it, I don't think it's going to make it.

All right. We have three minutes left. Staff, what should we be saying? Where do we land? Okay, next steps. Staff will make the changes that they can make based upon the discussion today. We are going to keep working. We'll have another round of reading next week. Hopefully not too many more comments and hopefully not comments backwards from the place where we landed back. But if they are, they are. We'll do our best to deal with that. Please get those in by the 16th so leadership has a chance to digest them. Our next working group meeting is July the

20th. At this pace, we are most certainly going to keep our July 27th call unless we happen to pick up the pace dramatically. Everybody, as you make a comment, and even as you go back through the comment you've already made, please ask yourself whether or not you are relitigating something or introducing a completely new concept into a very, very late stage document. That's not the point of the preliminary report. We've seen this language for weeks and weeks now. Most of it has been long stable. So, we really need to focus in on getting the report done. We have one minute left. Feodora, it is yours.

FEODORA HAMZA: Thank you, Paul. This is Feodora from ICANN Org. Just to note something in terms of when reviewing the draft initial report. The working group, it's at your discretion, but what might have caused confusion is striking each other's language proposals or resolving comments that were not uniquely yours. So maybe just try to make suggestions in the form of comments to keep the overview a bit cleaner. But just as a best practice, something to help the others. But whatever works for you. Just to note that.

PAUL MCGRADY: All right, Feodora. Thank you. Thank you, everybody, and we will take this up next week on page seven. All right. Thank you. Bye-bye.

DAVID HUGHES: Very small.

GABRIEL ANDREWS: Thanks.

[END OF TRANSCRIPTION]