JULIE BISLAND: Good morning, good afternoon, good evening, everyone. Welcome to the DNS Abuse Mitigation PDP 1 working group call taking place on Monday, the 1st of June, 2026. This is Julie for the recording. For today's call, we have apologies from Claire Craig, ALAC, Bruna Santos, NCUC. The alternates replacing them are Eunice Perez Coelho, ALAC, and Emmanuel Vitus, NCUC.

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 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. And with that, I will turn it back over to you, Paul. Thank you.

PAUL MCGRADY: Thank you, Julie. Good morning, everybody. Welcome to our last meeting before we all head to Spain. That's exciting.

First thing in our agenda is a welcome. We did that. Secondly, let's talk about some ICANN 86 prep.

All right. So we are in week one of June, in advance of ICANN 86. We are going to start deliberations on questions eight and nine, and prep for ICANN 86. So that's great. That way we will have touched every question before we arrive together. And in ICANN 86, we have four working sessions. None of them are public updates. We did that in the ICANN prep week webinar phase. So we will be working the whole time we are together in Spain. The sessions are staggered so that we don't get too sick of each other. And we can also go back to, I guess y'all can go back to the organizations that sent you, get feedback on what we're doing. So we have session one, Monday, June 8th. It's at 11:45 AM in the morning, and goes for a decent little chunk. And we are going to discuss a straw proposal for charter questions eight and nine. Those will come out of our work today. On Monday, we'll review unitary language for all the charter questions one through nine. We have then time on Wednesday to continue that because it's going to be a decent chunk of work. And we will be going into our cannot live with language. If there's something in here that is just a bright line no. Seems like it would have come up by now, but if not, June 10th is when we'll hear those. And then on Thursday, we will review the scoped impact assessment, and to the extent that we still have can't live with discussion going on, we will pick that back up after we look at the scoped impact assessment. So, that's what our ICANN 86 looks like. So it's going to be a good amount of work spread out over several days. So it'll be good to get together.

So what does that mean from the working group? We need for all of you to review the preliminary recommendation docs, and identify any areas that you cannot live with before June 8th, so that we have an agenda for that session. Staff will share the scoped impact assessment

on human rights and data protections on the current preliminary language with the working group today. Working group to review that before June 10th. And then we need for folks to identify areas of concern, feedback, or questions, so that we can add those to the discussion for our time together in Spain.

All right. So let us jump in. And charter question eight. It's a blank slate. What metrics will be used to evaluate the policy's effectiveness? We have early input themes from the SOAC, SGs, and Cs. There's links here to click on. I think these have been in the collaboration document for a while though. The early input themes is that there's broad agreement that the policy should be evaluated using real-world tangible measures that are generally outcome-oriented rather than abstract commitments. The IPC, ISPCP, and BC all offer concrete quantitative metrics, and the GAC proposed OCTO as a party that could measure data abuse trends. There is some slim alignment that quantitative measures alone are not sufficient. NCSG supports accuracy, proportionality, and process quality. While the ISPCP and BC emphasize campaign disruption, reducing uptime, and recidivism reduction rather than quantity alone. There is some variation as well between process safeguards raised by the NCSG, proactive identification raised by the IPC, and hybrid proactive identification and downstream impacts by the ISPCP and the BC.

All right. A number of pivot investigations. Here are some things, some early input suggestions. Here we go. Number of pivot investigations initiated per reporting period, number of associated domains identified, number of domains suspended, transferred, or otherwise actioned as a result. The framework should specify a review cycle, for example, every two years, at which aggregate metrics are assessed and the framework

adjusted if evidence of systematic over-enforcement or ineffectiveness is identified. Should look at the average reduction in abuse uptime. Some suggest the number of associated domains mitigated per confirmed seed domain. Percentages of confirmed seed domains that resulted in associated domain checks. Recurrence rate of DNS abuse associated with the same registrant account. That the metric should focus on the number of additional domain names being used for DNS abuse that were identified by registrars without having to wait for a report of DNS abuse. Increasing the number of associated abusive domains identified and acted on. Decrease in recidivism rates for registrants and customers previously found to engage in DNS abuse. In other words, fewer new abuse domains registered by the same entity. All right. I have a hand from Feodora. Feodora, go ahead.

FEODORA HAMZA: Thank you, Paul. We just wanted to provide context on this list. This is what different groups have included in their early input, and we have just put it here on list for the group to react to. It doesn't mean necessarily that everything is feasible or needs to be included. It's for the group to discuss what would make sense. So just to add that caveat. Back to you, Paul.

PAUL MCGRADY: Yes. This is the Christmas list from various groups in their early inputs. Yep. All right. And so those are the inputs. That takes us back to the question: what metrics will be used to evaluate the policy's effectiveness? This is the part, since it's our first look at this question,

where I just open a queue and people say whatever they'd like. We hope it's about question eight. All right, so let's get started. Reg, go ahead.

REG LEVY: Thanks. Can we have the list back on the screen? Thank you.

So there's a lot of registrant-related metrics, which I think are sort of the low-hanging fruit. If a registrant is identified as having conducted DNS abuse, then making sure that that doesn't happen again would be a good metric to go by. A lot of the others seem to indicate that there always are associated domains, and so if they are not found, then it seems that the associated domains check has failed, which I don't think is necessarily something that can be assumed. And others rely on knowledge or a broader understanding of the campaign.

And I'm just curious how it is proposed that ICANN or even a registrar would identify that a particular domain might be part of such a domain. Excuse me. It's early for me. Part of such a campaign. And I'm just wondering how that's going to be evaluated.

PAUL MCGRADY: Thanks, Reg. Volker?

VOLKER GREIMANN: Yes. Thank you. And I agree with Reg, but looking at that list, I have a lot of questions. The first point seems to indicate that we would have to entertain a lot of paperwork and documentation of the investigations

that we initiated, maintain logs of that kind, and basically put a large burden of documentation on registrars that would allow us to output those metrics. So I'm a bit cautiously pessimistic that that is feasible.

The review cycle is fine. The question though, for me is, what does this actually result in? If we have a review cycle that sees that there's no effect or no positive effect or even negative effect from this work, then what would be the outcome of that? As opposed to, if we find that this worked excellently and we achieved all our goals.

The reduction in abuse uptime is probably very hard to measure because obviously we're looking for domain names that have not been even reported yet. So how can they be measured in uptime versus... Normally, uptime is measured in when the abuse first got live or was first seen to when it was taken down. And that's a metric that's probably impossible to measure, at least in my experience. And the list goes on. I'm not going into every point, but I think each and every one of those ideas, which I absolutely support in the general principle will need to be tested and reviewed from a practicality perspective. Thank you.

PAUL MCGRADY: Thanks, Volker. Jothan?

JOTHAN FRAKES: Oh, yeah. You know what I don't see here, and this is, is it based on new registrations or just domains under management? There are some

registrars that grow a lot, some don't. Some have more new registrations and churn, some don't.

It's an interesting thing to understand what is going to be something that would be an indication of the benefits of this or how to do that measurement. And apologies, it's early on the West Coast. Hopefully, that was cogent. Thank you.

PAUL MCGRADY: Thanks, Jothan. Gabe.

GABRIEL ANDREWS: Hi, all. Gabriel Andrews with the GAC. One of the questions that I would like to see us be able to iterate on, and we don't necessarily know how to phrase this up front, but we were asking for, at least the GAC was asking for, I guess, or signaling opportunity for organizations like ICANN's OCTO to chime in with their studies over time. Further, I'd like to enable ICANN compliance to chime in after this policy's been in effect for an undetermined period of time, whether it's six months or one year, or what have you, to be able to come back to, whether it's this group or a similar group, and say, "Hey, this is where it's working for us," or, "Here's where we're having friction in even determining whether associated domain checks are being conducted in the way that we contemplated."

Right? Because if there's, for whatever reason, some policy gap that we don't contemplate now that prevents compliance from being able to go in and ensure that these checks are being done in the way that we hope

that they're to be done, I'd like to be able to iterate and adjust accordingly. So just wanted to raise that as a point of contemplation. Don't know what that text would look like, but just ensuring that we're considering that sort of iterative adaptability in the future. Over.

PAUL MCGRADY: Thanks, Gabriel. Yeah, it won't be this group because we will have handed in our recommendations and gone on our merry way, but it may be that after six months or a year, there is a report to the council, and they can determine from there what to do with that information. So we should capture that. There's a suggestion of a proper review of this two years in. Would like to hear some people talk about whether or not that's the right timeframe. Mark, go ahead.

MARC TRACHTENBERG: I think I'm with Volker on this one. I think conceptually a lot of things seem good, but first of all, I just think that this is going to be the greatest challenge possibly of the PDP of how do you figure out a way to measure anything that is meaningful? How is the data collected so that it's available for ICANN? How does ICANN get the data? What is done with it?

Just looking at some of this, number of pivot investigations initiated per reporting period, number of associated domains identified. It's like, compared to what? What is a good number? What is a bad number?

The average reduction in abuse time. Again, I think I don't know how you measure that. Who knows? How do you know when the abuse

started, right? I guess you could go back to when the domain was registered, but did it start then? I don't know. Number of associated domains mitigated per confirmed seed domain, compared to what? How do we know whether you caught them all? There's nothing to compare it to. Percentage of confirmed seed domains that resulted in associated domain checks. That one should be 100%, I guess, if the trigger is one abusive domain name.

Increasing the number of associated abusive domains identified and acted upon. It's like, again, compared to what? So I'm not trying to kick mud on this, I just, this is kind of the concern I've been saying from the beginning of how do we measure any of this stuff? And while conceptually I think all these things are good, I just don't know how you could get any meaningful data from it, and especially going after the fact, without having a gigantic obligation to collect a lot of data on the front end. I just don't know how any of this would be meaningful.

PAUL MCGRADY: Yeah. Thanks, Mark. And again, if anybody is listening whose bullet points here are laid out, I'll probably get nasty emails or whatever. But part of my job is to take a look at what we're looking at and see if there's a path forward in synthesizing things as I hear people talk.

And the theme that is coming out to me early on this, which is these are interesting data points, but there is no data pool right now. Right? And so we don't know if having zero pivots is normal, if having 1,000 pivots is normal, right? There was some talk about OCTO. Maybe OCTO has that data, and registrars are feeding it to them now. And there's some data

pool that we can draw from. But if there is a data pool, I'd love to hear about it and hear about what's in it.

But until we know that a registrar having zero, finding zero associated domains is for sure an outlier and that there's something weird going on there, or a registrar finding 10 times as many as the next registrar is an outlier and there's something strange going on there, I just don't know how we know what to do with any of these things, right? So for example, if you have the number of associated domain names mitigated per confirmed seed domain. Well, if we just say, "Okay, well that number should be 10," we just pull it out of a hat. Where do we come up with that number? And what happens if your domain name abusers aren't particularly abusive, right? And they only have six. Then you're a bad registrar because your domain names aren't particularly abusive. I don't know what to do with all this. So maybe there's a data pool. If there is, let's hear about it. Maybe some more ideas about maybe how we start to develop that data pool if we don't have it. I'm just trying to get us talking. Reg and then Gabriel.

REG LEVY: Thanks. Yeah. There's some conversation in the chat about asking OCTO about whether they have data in this regard, and that may be helpful.

I think part of the issue, and I understand and support looking for data-driven ways to identify this kind of thing. Excuse me, identify whether or not we've been successful. But I don't think there's a lot of good data, unfortunately. And, again, assuming that any particular domain is going to have X number of domains associated with it is not the right way of

going about it. And looking at the campaigns as a whole, that isn't necessarily something that a registrar specifically would have access to.

So while it might be worth saying we will know that this policy has been affected by comparing suspension rates of a registrar against length of time of a particular campaign, I don't necessarily think that that would be a reason for a breach if a registrar had not hit those metrics that it's not aware of.

I was going to say something else, but it has left my brain, so I will stop.

PAUL MCGRADY: Thanks, Reg. Gabriel?

GABRIEL ANDREWS: Yeah. So two things. One is, I don't think that I or others acknowledge Volker's point about collecting or there being this notion that maybe additional data has to be collected. And I'll just say that, at least from my perspective in listening to GAC feedback is I haven't heard from the GAC at this point any desire to add on additional data collection requirements above and beyond what's already being done for tracking how you handle abuse reports. So, I think that your point is well understood, that if you inject a lot of additional paper requirements, that could be counterproductive, and I just want to acknowledge the point.

Further, I want to agree and acknowledge with Reg's noticing that in the chat there appears to be a fair bit of support for the notion of asking OCTO to weigh in specifically. I'm thinking folks like Samaneh who are as

skilled researchers in ways that we are not to chime in at some point with a skilled analysis of whether and how and to what degree this policy has had a measurable impact in a way that I think those on this call maybe don't feel comfortable doing ourselves. Over.

PAUL MCGRADY: Thanks, Gabe. We have Ching.

CHING CHIAO: Thank you, Paul. This is Ching from the BC. I would like to echo what Gabe and Reg were saying, and I believe that for this particular policy input, this is not about domain operation or in any of the domain name life cycle. This policy is adding abuse, kind of a pre-medication time of work.

And so in principle, we shouldn't add any, like what Volker was saying, not additional paperworks on top of what registrar is already doing. And then I think to answer or to address this particular charter question, probably just for us to list all the possible items and then for either OCTO or the compliance to look at the list of possible areas of efficiencies of possible area of improvement for midterm or the longer term. We shouldn't put it as a kind of a require data input for all the registrars. Thank you.

PAUL MCGRADY: Thanks, Ching. And I put the question back, the question we're actually talking about back in the chat, which is, and this goes to Reg's point,

right? That this is not about evaluating registrar compliance, it's about evaluating the policy's effectiveness.

So I think that is important way to frame this, right? Oh, did I just get very quiet? Am I back? Okay. My computer's so weird. Thank you.

And so again, this is about the policy's effectiveness, not about registrar compliance. I think there are things that could be learned from that, right? Like if we have on average 8.76 domain names, additional domain names, uncovered, and we have a registrar that's uncovering zero consistently or 500 consistently, there may be things going on in that registrar's operation that compliance may want to chat with him about, but that's not the same thing as evaluating the policy's effectiveness.

And so when we think about the data we're going to collect, we need to collect data about that, not collect data about trying to pin something on a registrar. It's just not the question that we've been asked to answered. Thomas.

THOMAS RICKERT: Yeah, I think there's no way for us to come up with good metrics with ICANN's own resources or the registrar's own resources, because I think Reg made the point earlier that it's not necessarily telling if there is zero ADC required, because that basically shows that everything's in good order, that there are no abuse reports. So I think that when it comes to showing the effectiveness, we need to bring in OCTO and maybe others. But maybe OCTO is an excellent starting point to let us know what external players, be they commercial or non-commercial, can help

assess the overall landscape and tell us whether the policy moved the needle.

PAUL MCGRADY: Thanks, Thomas. Other comments on this? All right. Any objection to OCTO weighing in on this, but we don't want them to slow us down. That's the problem. ICANN staff of every department, I love you, but sometimes when we make ICANN staff's inputs a dependency, we lose weeks or months. So let's talk about what a controlled intervention by OCTO would look like, and maybe people who know OCTO better will have more to say. Thomas, is that an old hand or a new one? Old. Gabriel.

GABRIEL ANDREWS: Yeah, just to be clear, at least my understanding of this was ICANN OCTO weighed in after policy is put forward to measure the impact, not asking that they need to do any sort of report to us beforehand that might slow us down. At least that was my understanding. If others understood differently, I invite you to correct me.

PAUL MCGRADY: Got it. That's an important distinction. Is anybody talking about OCTO intervening now? Thomas.

THOMAS RICKERT: If the metric shall be part of our response to counsel, then I think we should ask OCTO earlier to advise on what external sources might be valuable for this exercise.

PAUL MCGRADY: In other words, if OCTO is the measurement outfit later, what data do they need from us to have the ability to measure it later? I think that's a legitimate question.

THOMAS RICKERT: Just a quick two-finger pause, if I may.

PAUL MCGRADY: Well, Thomas, can I strictly enforce my rule? Sorry. I'll come back to you.

JOTHAN FRAKES: Go ahead and let Thomas finish his thought, if you would. You got two wild boys here. Apologies.

PAUL MCGRADY: I got a rule breaker to help me let my rule breaker break the rule. All right. Thank you, Jothan. That's all right. All right, Thomas, you go ahead. Jothan's a darling. All right, go ahead.

THOMAS RICKERT: No, it was just because you responded to my point, and I'm not necessarily saying that OCTO shall be the entity conducting the

measurement ultimately. But I think it would be good to hear them in terms of who could be helpful with that. Maybe they say it's something that they can't do with their own devices. Maybe they say that they can't do it for resource or other reasons at all, and I think that's something that we should know so that we can bake their response into us reaching out to other third parties or leaving it with OCTO.

PAUL MCGRADY: Thanks, Thomas. All right, Jothan, go ahead.

JOTHAN FRAKES: Yeah, and Thomas was actually helping me make my point. The other thing, I won't repeat what he said, but one of the things that we really should do is if this measurement is happening and information is coming from OCTO, that we make sure that it's specific to the defined areas of DNS abuse that are commonly used. One of the challenges in combating DNS abuse that I notice is that there's categories of DNS abuse that fall in the content realm that are not related to the defined DNS abuse as we work with them. The four plus one as it relates to the four definition that we're using as an industry currently.

And one of the challenges has been normalizing that, so that everybody's working with that same shared definitions. I think that measurements are going to be unuseful if we're not all using those same definitions. And that's something we need to probably factor into this, that it's going to be phishing, malware, blah, blah, blah. And that needs to be defined. If it's just pure spam or some of the uncategorized things that don't fall into the DNS abuse definitions, those could be

miscounted or could be bad calculus. So we want to make sure that OCTO is working from the same script. Thank you.

PAUL MCGRADY: Thanks, Jothan. Anything else on this? Okay. Oh, Farzaneh, go ahead.

FARZANEH BADII: Sorry, Paul. I just wanted to say that it seems to me we need to know what OCTO and DomainMetrica is providing, what sort of data it's providing already, if that data can be of use to us, and to measure the effectiveness of the policy and then ask for them to also do a presentation if we want to involve them further. But I think the first step is to actually know what they provide in DomainMetrica. Thank you.

PAUL MCGRADY: Thanks. Brian?

BRIAN CIMBOLIC: Sorry, I always have microphone duties. My first Zoom of the week. So I put something similar in the chat, and it doesn't necessarily get to the policy's effectiveness once implemented, but I think there's value in a sort of proof of concept to show why an associated domain check would be so important. And that would be if any registrar that is already doing associated domain checks could kind of put forth a case study and say, "We discovered a domain engaged in phishing," and then upon conducting an associated domain check, checking the account, we saw Y

number of domains that were also engaged in a similar, oftentimes, for example, let's say a toll road scam. They discovered one easypasslogin.tld, and then there were 40 other in the account. That sort of anecdote, while not quantitative, I think itself sort of shows the importance of the ADC, which I think could actually help be an input in response to this question.

PAUL MCGRADY: Thanks, Brian. Reg, go ahead.

REG LEVY: Thanks. Yeah, and in response to Brian's request, I don't have a case study on hand, but anecdotally, we rarely see this, right? So when we do conduct ADC checks, it is frequently the case that that account does not have anything related to it.

When we have successfully identified issues that involve campaigns, it's on the basis of a fraud situation. And so we've identified that because there was a particular credit card that failed, and then we look at that account, and we see that they were used for a whole bunch of different things.

And to the point of large-scale campaigns, I think that NetBeacon has a significant amount of data that shows that this is across registrars. So it seems that there has already begun to be a pivot, I keep losing my hair, that there has already begun to be a pivot by DNS abusers away from using a single account or even a single registrar. And so I'm very concerned that we're already late with this idea, and that we're

spending a whole bunch of time and effort, and we're going to end up with a policy, and two years from now, we're going to have OCTO run a review and find out that DNS abuse has not decreased, but we have successfully decreased DNS abuse targeted at single registrars. And I see support for that from NetCraft in the chat, one of the reporters that we trust more than some of the other reporters.

PAUL MCGRADY: Thanks, Reg. Ching?

CHING CHIAO: Oh, thank you, Paul. I totally agree what Reg was saying. I think we're already late in the game, and then the policy focus on single registrar working on ADC. So if we're talking about large scale, once again, the campaign itself, having one single registrar making the report doesn't make any... I mean, can be part of the picture, but it doesn't make the full picture for the campaign. So, let's just be reasonable and also be realistic for this particular question. Thank you.

PAUL MCGRADY: Thanks, Ching. We have Gabriel. Go ahead.

GABRIEL ANDREWS: Yeah, just responding to Reg, and also I note in her chat window two things. She's asking if we even need this policy in light of what she just said, and I want to acknowledge that what she said is very much what my understanding of the world is, is that the bad actors will adapt to

what we do, and they already are sometimes, as she indicated, using multiple registrars, which, yeah, that's happening. They're also sometimes using a single registrar as much as possible until they're kicked off of it, too, right? And so that's more cost efficient for them, especially if that registrar is cheaper than the other ones they prefer not to use. And so part of the policy that we're doing is to increase the cost of doing harm, the cost of doing the abuse to those abusive actors.

And that itself is worthwhile, even if it's not perfect. Worthwhile. Although she is quite correct that eventually at some point, we as the community are going to have to contemplate how cross-registrar sharing of threat indicators might be contemplated, and it's something that's a discussion that's happened a little bit and then come back to. I don't see it as being in scope to this conversation, but I think it's fair to recognize that that is a conversation that might have to happen. But I think that that will absolutely require this to be in place first. That's at least my understanding of things. You can't really expect there to be that cross-registrar communication of threat indicators if you aren't first ensuring that when a bad actor is abusing a single registrar, that's handled. So those are my thoughts in reaction to Reg. Over.

PAUL MCGRADY: Thanks, Gabriel. Feodora.

FEODORA HAMZA: Thank you, Paul. Just to note that in the charter under deliverables, there is a little bit more input on this, on what could show effectiveness of the policy. So it doesn't necessarily just have to be the exact kind of

data in the, like, for registrars, but also some other potential considerations. I can put it in chat, but just wanted to note it might not always be technical and just to check the charter again. Thank you.

PAUL MCGRADY: Thanks. And everybody, she's talking about the data and metric requirements on page five at the bottom. Brian, go ahead.

BRIAN CIMBOLIC: Thanks, Paul. So I think Reg's point is well taken, in that there are, obviously campaigns aren't necessarily only isolated into individual registrars. They can be spread. But as Reg mentioned, also too, the NetBeacon data, I think, does bear out month over month that you do get concentrations in handfuls of particular registrars. And you will oftentimes see when you're looking at individual campaigns, toll road campaigns or the winter fuel campaign, they really were concentrated in a handful of registrars.

So I think that the associated domain check, sure, it might not be a perfect solution, but if there is no perfect solution to DNS abuse. And so I understand that it may be an imperfect mechanism, but we're never going to have a perfect mechanism for DNS abuse. And each element that we add friction and makes it harder, sure, the bad guys are going to change their tactics, and then the next PDP, they'll change their tactics again. It's not our job to say because they may change their tactics, we just kind of throw up our arms and give up. I think that this is a worthwhile endeavor. I think that it really will have an impact, particularly on those registrars with super, super concentrated levels of

abuse. That's where campaigns are happening, and this is where I think that the policy can be really disruptive for those registrars.

PAUL MCGRADY: Thanks, Brian. Volker?

VOLKER GREIMANN: Oh, I absolutely agree with everything Brian said. We see it in our registrars, how effective this is, to do the check for domains where it makes absolute sense, where we have the experience that there might be more, that when we conduct the check, that we will usually find at least one or two other domains, but sometimes even hundreds of domains that have not been weaponized yet or that are going to be used for similar campaigns, sometimes even other campaigns. So, these checks absolutely have value. I just feel that we need to be careful in how to frame the entire thing to make sure that we can carry on efficiently in doing our work. Yeah. Efficiency, I think is my main focus here.

PAUL MCGRADY: Thanks, Volker. Luke?

LUKE WOOD: Yeah, definitely agree with Brian about his points. Luke here from Netcraft for clarity. We definitely do see abuse clusters across registrars. It is a smaller volume typically to our typical abuse of domain registrations we detect. So whilst it does exist, it is still an emerging

area. So definitely agree with Brian's point. Most of those existing campaigns are on a few registrars and specifically one registrar typically. So definitely still think it's worthwhile PDP, but just adding my two cents. Thanks.

PAUL MCGRADY: Thanks, Luke. Okay. We're at time on this, but if there's more to say, let's say it. I see in the chat Reg has put in things that I'm assuming that Reg would like to measure, false positives, legitimate domain names wrongly actioned, accuracy of association, pivot correctness, and proportionality of enforcement. Reg, do you want to speak to that? And I think from the mirror of that obviously is important too, I guess, right? Correct positives, correct pivots, and something, I guess proportionality of enforcement is itself a mirror, right? It's what a proportion means. But Reg, go ahead.

REG LEVY: Yeah, thanks. Can we go back to the bullets? Thank you.

So, these are good ideas, but they only measure in one direction, and I think it's also important to measure in the other direction. So not just how many domains were recognized with regard when somebody said a seed domain, again, making an assumption that every abusive domain has related domains is problematic in itself. But if we take that assumption, then making the case that, okay, for every one seed domain, X number were identified. It should also be determined whether or not that identification was correct.

So if we're going to be assuming that every domain is guilty, then we should look and see what the impact is about suspending non-guilty domains.

PAUL MCGRADY: Thanks, Reg. Before you go, since you said some of these are good ideas, are there any on here that are, from your point of view, that are bad ideas? I have a couple on here that I think are bad ideas, but I'm trying to try to let the conversation free flow. Some of these are good data points, but some of these seem more trouble than the others. Do you think?

REG LEVY: Yeah. So I think that the very first one, number of pivot investigations initiated per reporting period. So first of all, that's going to depend on the volume of domains of a registrar. So a registrar with 1,000 domains per reporting period versus a registrar with 10 domains per reporting period are going to have very different numbers of pivot investigations. So, raw numbers I don't think is a reasonable way of looking at this.

The review cycle with regard to-- I mean, basically, I have issues with all of these because we don't have the data, and there's not a real way for the registrars to have that data unless you're going to require us to purchase that data from DNS Abuse retail block lists. So yeah, I have issues with a lot of these. I understand the direction in which that we are going, and I do support data-driven results. But I don't think we have a lot of data.

PAUL MCGRADY: Thanks, Reg. And I think maybe it comes down to an issue of timing, which is why the two years is in here. Like I said earlier, we don't have a data pool now, and so we don't have any way that I can see from day one to evaluate the policy's effectiveness on day one. That may be different if we identify data points that we think are a good idea, data points that then go from the registrars to org that Octo, I suppose, looks at, and after two years or so can tell us whether or not the policy's effective.

But effectiveness on day one or even month three, I think is going to be hard to do. There was some talk about a report at month six. Maybe there's enough data by that point, I don't know. But we're data poor now. We may not be in two years, but we need to identify what data points we actually are going to collect and send. And so we have to ask ourselves whether or not each of these is a good idea or a bad idea, or as Volker would say, efficient. Are they actually reportable without creating an entire new thing?

I'm going to do it anyways. I'm going to get a nasty email. I don't know how to measure recidivism rates for registrants and customers previously found to be in DNS Abuse across all registrars or across the individual registrar. What is that even like? Does that make sense? And so I don't think all of these ideas are born equal, and so I think maybe we need to have a good idea, bad idea exercise as we look at these bullet points. I'm talking out loud now, and I'll probably regret saying that. All right, Farzi, go ahead.

FARZANEH BADII: Thank you, Paul. Actually, so what NCSG has been saying since before the start of this DNS Abuse Mitigation group is that as well as quantitative indicators, we need qualitative indicators. But what we mean by qualitative indicator as well as having some metrics that is not just based on numbers, we also mean qualitative indicators that show how using this ADC impacted, like as Reg is saying, if there are false positives or disproportionate enforcement.

Because if we come up with a policy that is even effective in mitigating abuse, at the end of the day, mitigating abuse and reducing abuse, but it affects people and innocent registrants, that policy is not a good policy. Because at the end of the day, we can, of course, jail all the criminals or have capital punishment, but that's not a good policy.

And for the recidivism, honestly, in criminal justice studies, there are so many factors that are involved with recidivism, and it's very hard to measure. And also most of these metrics, there is going to be weak correlation. I don't see how we can have a strong correlation. And to your point on, like Yao has commented on a few things that we need to be very careful about and criticism on some of these metrics that I think in chat that I think is worth looking back.

PAUL MCGRADY: Thanks, Farzi. All right. We are already over time on this topic, so I'm going to call for final hand raise. I saw Michaela. She went away. Come back, please, if you have something to say.

I don't see any additional hands, so I'm going to draw the line after Miche-- Oh, Feodora. I'll draw the line after Feodora, and then we'll move on to the next charter question. All right, Michaela.

MICHAELA SHAPIRO: Thanks, Paul. No, just a few small points and really echoing the qualitative indicators that Reg shared and plus one, plus whatever to all the comments that Farzana just made.

I also wanted to comment on the point that Brian put in the chat about, let's say a registrar gets a lot better and is having less abuse in the first place. Overall, over time, it'll have fewer EDCs. I think that point is really important because we don't want to create a policy that through this, however we're trying to get to the policy, we don't necessarily want to reward more EDCs conducted or more EDCs found is necessarily always a positive or a sign of success is the number of takedowns or however terminology we want to use there. So just, I think, an important caveat to keep in mind.

And there was a point by Nick as well about ICANN compliance and a record of complaints and wrongly applied domain suspensions. I wasn't able to attend that webinar, but if they do have data on that, that would be fantastic. If they don't yet, maybe that's something that could be explored further. So just excited to see that suggestion in the chat. Thanks.

PAUL MCGRADY: Thanks, Michaela. All right, Feodora.

FEODORA HAMZA: Thank you, Paul. Just to summarize, and as you noted earlier in the slides, we will take everything that was discussed today and develop a strong proposal based on the input we received from the group. And we will also inquire with our colleagues to see if we can get more feedback. Some suggested to discuss with Octo, and by Monday, we should have more structured input to help the group potentially come up with a full answer on this. Thank you, Paul.

PAUL MCGRADY: Thank you. Okay. I think that's Feodora's gentle way of saying, "Move on." Let's move on. Charter question number nine. And I'll read the charter question, and then Feodora has some early inputs she wanted to share. So the question is, how can registrars demonstrate their compliance with the obligations to ICANN, and what types of evidence and information can registrars submit? And, Feodora, do you want to run with this?

FEODORA HAMZA: So this one is for you. The next one would be for me.

PAUL MCGRADY: Got it. Okay. So from the early inputs, which have been in the collaboration document for a bit, the input largely agrees that registrar compliance should be demonstrated through a good faith process rather than outcome-based guarantees. Multiple groups emphasize procedural evidence and a reasonable investigation process, while

other, BC, NCSG, ISPCP, and the registrars points to this existing already in the RAA.

There is broad alignment on documentation and record keeping, including logs, documenting steps, and record retentions for audits. There's also convergence that transparency and accountability can be achieved without disclosing personal information. There is a divergence in the level of evidence required and whether this is already covered in the RAA or requires new policy.

So that's the early inputs from all y'all, as we would say. And now we have some good stuff from Feodora. Go ahead.

FEODORA HAMZA: Thank you, Paul. Hi, everyone. This is Feodora from ICANN Org. On this slide, you see some input from the current compliance practices regarding the DNS Abuse Contract amendments or obligation.

What is important for the group to discuss, or when discussing this question, that the method for demonstrating compliance would likely follow the same principles as today for the other DNS Abuse related requirements. So registrars typically demonstrate compliance by providing information and documented evidence that shows what actions they took, when, and why. So in this case, or in a best case scenario for demonstrating compliance, would be a clear auditable, sorry, record that matches the language of the obligation.

So evidence might include logs, investigation notes or, these are just illustrative, or ticketing system entries showing that a required review

or action was performed or acted upon. Again, just an example. So the exact form of evidence would very heavily depend completely on how the obligation is drafted. So saying it ultimately compliance can only enforce and can only require documentation of what the RAA itself will state or say.

So I guess what this means for ADC, and this is what the group has to discuss further, is do the preliminary recommendations reflect those principles? And yeah, are the ADC requirements that the group has discussed so far precise about what counts based on the charter questions as an associate domain, reasonable investigation, and what minimum steps registrar must take in this case? So that was the input from our side. Hope this helps, and back to you, Paul, to managing the group.

PAUL MCGRADY: Thank you. All right. We have a healthy queue already. We have Marc. Go ahead.

MARC TRACHTENBERG: I guess I'm just going to make a comment that I've already made several times at this PDP before, which is just looking at this and looking at the underlying language of how compliance enforces the requirements of DNS Abuse. I think one of the main ways, if not the main way, is through external complaints, which are not going to happen here.

That is not practical because unlike DNS Abuse, where people report it and they can determine whether or not action was taken by the

registrar, and not even always, like sometimes the domain sinkholed, you can't tell whether it was actioned. But in general, there's some indication of whether action was taken or not, which can drive external complaints to ICANN. That will not happen here because there is no transparency. There is no way for the external reporter to know whether or not the registrar engaged in ADC or what kind of ADC it engaged in.

So the only way that any sort of determination can be made whether registrars are complying is through regular audits. That's just a practical reality. And so that means there has to be something for ICANN to look at if they do these regular audits, and what will those things be? And those things can only be various records, and there is a risk it just creates a lot of obligations to create all these additional records that don't exist now. And even so, I don't know what those records would include that would be meaningful for ICANN to even look at. So this is another gigantic challenge for the meaningfulness of this PDP.

PAUL MCGRADY: Thanks, Marc. All right, Volker?

VOLKER GREIMANN: Yes. Thank you. I'm not going to say the word again because I said it before, and we have our policy internally, so. But consider it said.

This has probably the largest potential for dispute in the entire working group. I think the baseline that we can probably all agree on is worthwhile and helpful is that each and every registrar needs to come

up with an internal non-public policy that can be presented to ICANN that details how ADCs are being conducted, what technical abilities and checks we have available, which ones of those will usually be triggered, which ones can be triggered in addition when we have certain cases that suggest there might be further information. So basically, a workflow document, policy document that ICANN can check against when looking at abuse complaints or as part of an audit.

I fully appreciate the concerns that Marc has that it cannot be checked on a basis of per domain, and that's an issue that even I, when I look at certain things, sometimes face when I look back at certain takedowns, when I try to figure out why did I take down this domain name again? Oh, this was a bulk update. Okay, then it was probably part of an associated domain check. But it's going to be very hard to find the tickets that led to that because it was probably for another domain.

Therefore, my proposal here would be that, A, ICANN has that policy to check against, and B, if ICANN gets multiple reports about certain connected domains that they will be able to identify either through Octo or through reports by reporters that specialize in these kinds of activities, and ICANN then determines that these should have been found by the processes that the registrar has described in his policy and has not found it, that might be an indication of non-compliance.

I think that would probably be the most lightweight and least bureaucratic way to approach this. Might cover the basis for what is needed for those that would like to see more enforcement and enforceability, and basically squares the circle. Yes, you might want more, but if you want more, you have to realize that more time will be

spent on each report and that time will go away somewhere else and therefore might have detrimental effects on abuse mitigation. So all in all, that would be my preferred outcome. Thank you.

PAUL MCGRADY: Thanks, Volker. Before you go, can I ask you a question, which is, if compliance will be based upon the registrar complying with its own internally crafted document, how do we avoid the problem of the registrars who don't want to do this crafting a document to make sure that they don't have to? Right? That's the whole point of having a policy that applies to everybody. How do we deal with that problem?

VOLKER GREIMANN: Well, the policy should probably have certain guidelines, certain rules that flow from the advisory that ICANN is going to create, i.e., there are certain minimum steps that will have to be taken care or alternative steps that will have to be taken care of. And ICANN would be within its remit to analyze that policy, suggest alternatives, improvements to that policy where possible.

When comparing policies of registrars, ICANN will probably have a better view of what is out there, what certain registrars have as a policy, and therefore also allow for an iterative process with each registrar to make sure that this is regularly updated, reviewed, and can actually lead to improvement. So that would be something that I would see as part of the advisory.

If it doesn't want to do it, then the policy would probably speak to that. If it says we are only going to do that and only when the moon shines thrice in full moon in the one month period, then obviously ICANN will be able to knock on that and say, "Look, that just doesn't meet the requirements."

PAUL MCGRADY: Thanks, Volker. All right, Anil.

ANIL KUMAR JAIN: Thank you, Paul. Anil for the record. Two things. Number one, when we are talking about compliance practices, we have already written in RAA, and it is already signed. Now, here question is that, once we are going to give additional advisory based on ADC, whether the existing RAA, we are intending to get it changed, or it is only for the fresh RAA, which we are talking about. This is the first thing which I just want to ask.

The second is that I think we can send an advisory. We can give an advisory to the registrar that whether it is a ICANN-based advisory on DNS Abuse compliance practices, or it is their own internal DNS Abuse practices. We may advise them to publish on their website so that the registrant and the users largely get impacted, and they should get confidence that this registrar is doing the right practices to protect them in future. Thank you.

PAUL MCGRADY: Thanks, Anil. Ching?

CHING CHIAO: Thank you, Paul. This is Ching. So I will agree what Volker was describing. And building on top of that is that, once again, we all know that ADC, potentially, especially in the large-scale campaign, will keep changing. So that is why we as a BC, as a group, we say that it should be a good faith reporting, it should be a good faith exercise.

But having said that, I think a necessary record-keeping, as Paul, you mentioned probably a couple meetings ago, that there will be data attached to what registrar will be doing for the ADC. Let's say, the timestamp for starting to conclude, we talked about that in the different charter questions. And then, once again, I mention also the ADC group size, some ADC group numbers, simply for the record keeping, and then for the ICANN compliance to have a record that the registrars are keeping good records of those ADC checks. Thanks.

PAUL MCGRADY: Thanks, Ching. Gabriel.

GABRIEL ANDREWS: Hi. So I just wanted to read and then reflect and expand upon some of the GAC feedback on this question, which is that the GAC would welcome feedback from ICANN compliance on how registrars can and/or should demonstrate compliance with this ultimate policy, as well as which evidence or information that they would require of the contracted parties. That's the statement.

Take a step back. Real-world scenario. Let's say that ICANN compliance is only involved because someone came to them and said, "Hey, we reported this domain that was abusive, and then a little while longer, we saw additional abuse from this other domain that looks like it's the same bad actor, same registrar, et cetera. We reported that one, and we're not seeing action by the registrar to pivot off of these reports to take action against the actors." That's the kind of example I would expect would elicit a compliance investigation. Doesn't mean that their allegation is true, just want to be clear on that.

But how is ICANN compliance even involved in the first place? It'd be something like that to have occurred. So if that were to happen, I would still think that it would be valuable for this group to hear from compliance what information they can ask for, to actually check, "Hey, you got multiple abuse reports. There's an allegation that an associated domain check should have occurred, and if so, that it should have detected this." Is there anything right now that ICANN compliance sees as an obstacle to being able to ask that question? And I'm not sure I have clarity on that, but I would like clarity on that. Does that make sense?

PAUL MCGRADY: Thanks, Gabe. Farzaneh.

FARZANEH BADII: I actually want, in a turn of event, I want to agree with Gabriel. We agree on many things. And I just want to say that, one way of actually proportionate compliance is to see how the reporter has some ways to

report that there's this domain name that has been abusive and for a long time, and what can be done about it. So I think, if we can further talk to compliance and see how that can happen, that would be good. But of course, it has some implications.

And also, I think that at this point, we need to talk about the enforcement and compliance of domain names that, what are we going to do with domain names that were abusive, but when they got the report, they stop being abusive, but to be later down the road to become abusive again. So how are we going to approach compliance about that?

I think that we have our opinions on that, which we have talked about, like we should be proportionate, and it should be based on actionable evidence, and actionable evidence should not go back to many years of a long-term abuse. But these are the things that we need to discuss in terms of the compliance and also transparency. Thank you.

PAUL MCGRADY: Thanks, Farzaneh. Reg?

REG LEVY: Thanks. In the example that Gabe just gave, it sounded as though there was a domain that was abusive, it was resolved, nothing got found, and then there was a new domain that was abusive. And so I don't see how this policy requires us to draw that inference over time. If the domain was abusive or potentially abusive and in existence at the time of the ADC, sure, maybe.

But I'm a little concerned that this is requiring us to constantly be on the lookout for a new domain that matched a domain that we suspended six months ago. And currently, ICANN compliance has very good ways, as far as I am concerned, of making sure that we are compliant with all of our requirements. And whenever there is a hint, a whiff of anything to the contrary, we are immediately assumed to be doing the wrong thing, and we have to prove that we have not. So I would like to assure everybody that ICANN compliance is extremely capable of enforcing these contracts.

PAUL MCGRADY: Thanks, Reg. Feodora.

FEODORA HAMZA: Thank you, Paul. This is Feodora from ICANN Org. Just to note what we said earlier, that the group maybe needs to check the current recommendations and see if those provide the information for demonstrating compliance, such as what actions the registrar took, when and why, in relation to associated domain checks, and determine if that could satisfy this question or if more is needed, taking into consideration the different language that the group has discussed in the other recommendations as well. But just to note that there might be some homework for the group here as well on this. Back to you, Paul.

PAUL MCGRADY: Thanks. Ching?

CHING CHIAO: Thank you, Paul. This is Ching from the BC. So I'm a little bit concerned and confused at the same time. So let me put it this way. So Gabe shared that example and then Reg framed this particular ADC should be conducted at the same time as the abusive domain is registered.

I'm concerned on one hand it's about if we're laying out too specifically on the timeline and then for compliance to execute based on the timeline or to audit. And I think this would give the potential bad intent actors just to try to dodge or try to stay away from the timeline and kind of to indirectly encourage the slow burn type of the campaign.

And yeah, so that's kind of the concern and the confusion I would like to share. Probably we need some clarity and, yeah, from just within the group or from the ICANN compliance to talk a little bit more on this. Thank you.

PAUL MCGRADY: Thanks, Ching. Marc?

MARC TRACHTENBERG: Just to respond to Reg's point on the effectiveness of ICANN compliance, I think their ability to investigate complaints is not the same thing as saying how good they are at enforcement, right? They're responding to complaints that they receive, and they have to investigate them. So I can't speak to how they act when they reach out to you, and if they are assuming that you're wrong. Maybe it's just based on the evidence that's in the complaint, I don't know.

But investigating a lot of complaints they get is not the same as enforcing the policy. And here we're not going to have any complaints. Not really. I mean, Gabe gave one example, and I like the specificity, so that's helpful, but I think it's really an edge case that's not going to happen very often.

So, I think there is a real question here of how ICANN can enforce this because, again, I don't know how much enforcement is really happening for other policy violations, especially when we have the same reports that we're submitting against the same registrars, and they're investigating those reports and maybe the domain name eventually gets suspended, but nothing happens with that registrar no matter how many reports we submit. So just a counterpoint.

PAUL MCGRADY: Thanks. I don't want to get too bogged down on how great ICANN compliance is or isn't. The question is, how can registrars demonstrate their compliance with the obligation, with the policy's obligation, I guess is what we're talking about, to ICANN, and what types of evidence and information can registrars submit? And I guess those eight and nine are grouped together on purpose because it seems like that evidence and information probably tracks directly to the metrics that we would collect under charter question eight. And so I want to keep us as focused as we can on trying to answer the question. Volker, go ahead.

VOLKER GREIMANN: Compliance works in the way that somebody has to bring a complaint, right? So if there's no complaint, then there's no compliance

investigation. Therefore, somebody will have to report to ICANN that a registrar has not met his obligation under the ADR policy that we are currently developing.

When that complaint comes in, then ICANN will conduct an investigation based on the evidence that is available. What evidence is available is usually the data of the original report and any additional reports that suggest that there may be more domains. Because the reporter will have to know from somewhere that there was more than one.

And based on that, and looking at the policy that the registrar has developed, the registrar can then look at the domain names that have been reported and see whether they would have been found if they had conducted the ADC under their policy. If that turns out that they would have been found under that policy, under the practices that are established, then there would be a violation or at least further investigation to justify why it wasn't found in this specific case, or remediating action.

If it would not have been found because of how the domains have been registered, it could have been that the check would not have resulted in the discovery. Just because they were the same campaign doesn't mean they have to have the same markers within the registrar. Then that would also be demonstratable to ICANN as part of their investigation. So I really feel that having a policy in place that I can check against and that the registrar has to operate under is the right way forward here.

PAUL MCGRADY: Thanks, Volker. I think Marc's point was that we can't rely on the inbound complaint process anymore because there's no visibility into how many domain names a particular bad actor has registered within your registrar. Back in the day, we did have access to data, and people were able to do those sorts of cross-checks across WHOIS data imperfectly, but at least there was something. Now, there is nothing. And so that's to the point. But as Reg points out in the chat, ICANN compliance does do audits. And so that's an important thing, and I think it should affect how we answer question number nine. Reg, go ahead.

REG LEVY: Thanks. In response to how can registrars demonstrate our compliance to ICANN, I would say in the manner that we currently do. My understanding was that there was not a requirement that we create new types of records. So that seems to me to be outside the scope of this. The types of evidence and information that we would submit are the types that we currently submit. Like I said, we've been doing this for a while. ICANN is pretty good at this.

So it sounds like what people want is for ICANN to come in, especially because the registrar is saying, "Trust us, ICANN does this very well," are not being believed. So I would like us to reach out to ICANN and say, "What you got?" I would, however, prepare you or recommend that you be prepared for ICANN compliance not to provide a response, because they very often resist responding to hypotheticals or putting input into policy, so...

PAUL MCGRADY: Thanks, Reg. And I see Farzi's commenting about my mentioning of WHOIS. I was not offering a qualitative opinion on whether or not the old WHOIS system was good or bad, but just saying that there used to be publicly facing data and now there's not. There is publicly facing data on DNS Abuse because you can go to a website and see it. And so that's the whole point of that, which is we can't rely on third parties reporting ADC check problems. Yeah. So anyways, but Farzi has forgiven me in the chat, so that's nice. All right. So, this was a good talk on this one.

And again, I don't want to get in trouble, and I don't want to be accused of reductionism either, but isn't a possible answer to question number nine that registrars keep a log of what they've done, and when ICANN does a regular audit on this particular compliance item, they produce the log? Is that an answer? Is that too simple? Yeah, if logs are kept, and so maybe there needs to be a requirement that a log be kept. And so I don't know. So Reg is against requiring a log. All right. So maybe I've started a firestorm. Let's see. We have a few more minutes. Volker, go ahead. And I expect to hear from Reg because I got a capital no.

VOLKER GREIMANN: Well, logs are being kept, but the logs might not be useful in this context. Of course, every transaction that we do with a domain name will create a log in our system. So if we set a domain name to client hold, that will create a log in our system. That log does not necessarily, or even by design, include any information why that domain name was set to client hold, because that information will flow from somewhere else, maybe from a ticket that we've received, maybe from having

recognized that this is an abusive domain name through other sources like an ADC.

And sometimes the log of why the domain has been suspended only exists in the head of the abuse mitigating officer or agent in our system. So, there's logs, yes, but those logs will not always have the data that you need. Therefore, I would be very critical of creating more new logs.

PAUL MCGRADY: Thanks, Volker. Before you go, if we say, okay, no new log, is it simply then just, but this happens, the data is collected? Data happens, right, when you do something like this, as you've noted. If you suspend a domain name or those kinds of things, is it simply just we say that there needs to be data retention sufficient to show compliance, and that's already part of the RAA, and therefore nothing else needs to happen?

Let's keep riffing on this, because if there's no new log and there is data being collected, doesn't the registrar want to be able to have data to show ICANN that it complied if they get audited? Keep talking.

VOLKER GREIMANN: Yes. So one thing that we want to do is handle abuse complaints, and we want to be able to handle as many abuse complaints as we can in the time that is available to us. And the more records we need to create for every complaint that we action-- of the steps that we've taken, of why certain steps were taken, and which domains these steps were taken with, the more time we will not be able to do other things when mitigating abuse. Therefore, I'm arguing against more logs.

Yes, it would be useful in certain cases to have those logs. However, given the fact that we only need those logs in maybe 0.01% of the cases where we take action, the efficiency... Oh, damn, I said it again. The word seems to suggest that it's rather a waste of time to make sure that these logs are there and focus on the actual work that we are doing. Yes, it is helpful to have logs. Sometimes it might even save you some time, but overall, it saves more time not creating all the logs that you might need to create manually. Otherwise, you're less the word.

I had a case where at the last contracted party summit, for example, I walked Marc through a case of an associated domain check where he reported the domain name to us, and we looked at the domain record together. We found one more domain name that was registered through the same reseller, same date, had the same naming patterns, and we took it down. That was basically a bulk command in our system where I took those two domain names down based on the one report.

The only record that was created at that time was that these two domain names were created at the same time, and that record is not easily visible in our database or our web interface. Therefore, it would require someone from the development team to look that log up. Development team time is very, very rare and very, very hard to get, especially for non-profit-making efforts like abuse report intake and mitigation. Therefore, the urgency is very difficult to impart to management sometimes that we need development times to just evidence something that we've done right.

I therefore would posit that, yes, while there are logs and while ICANN compliance might be able to look at that, and this may vary from

registrar to registrar again, and the process is used to do the takedowns, but we should always aim for the road of least impact and go with a way that allows us to work smoothly. Thank you.

PAUL MCGRADY: Thanks, Volker. Gabe, go ahead.

GABRIEL ANDREWS: Hi. So I just want to recognize and thank Brian for quoting the existing RAA text under 3.18.4 in the chat. Now, I don't expect people to find this. It's really hard to go back and find the chat, but I'm going to try to read what he posted here. From 3.18.4, and you can Google this on your own and read along if you want or find it after the fact.

But the existing obligation is that the registrar shall document its receipt of and response to all such reports. They're saying abuse reports. Registrar shall maintain the records related to such reports for the shorter of two years or the longest period permitted by applicable law. So when I hear that there's a requirement to document its responses to all such reports, is there anyone that disagrees? If you're required to document your response, that includes documenting whether or not an ADC was conducted.

PAUL MCGRADY: Thanks, Gabriel. Good question. Jothan, go ahead.

JOTHAN FRAKES: Yeah. Thank you. And I put it into the chat. We've deferred other parts of other questions related to being in scope or out of scope of this group's work because we're talking about detection and not necessarily what happens after that, whether there's mitigation action or other things happen.

And I wonder if there's pieces of this that we're assuming mitigation occurred and then we're assuming some kind of a measurement would have to happen based upon that fact versus detection, right? Which is what the scope of this group is. So I'm kind of elevating it to being we're having a discussion about what we detect and how do we determine how we can report to ICANN about the effectiveness of that detection. Thank you.

PAUL MCGRADY: Thanks, Jothan. Yeah, that's right. We're talking about what happens when there is a trigger, what happens during a reasonable investigation and what criteria were applied, right? And there may be, as Volker is saying, that your system may collect those automatically, so additional logging isn't necessary. Maybe not. I'm not clear yet on that. I see Volker back in the... I'm going to call on Marc first, and then we'll hear again from Volker. We have five minutes left, so anybody that wants in this queue, if you could put yourself in it pretty much immediately so I can parse out the time we have so we end on time, that would be great. And I do need to save a hot second for AOB for staff. Marc, go ahead.

MARC TRACHTENBERG: I think from this discussion and the background, it's clear to me that there is no way to demonstrate compliance

MARC TRACHTENBERG: with the policy without logs being kept. And before Reg freaks out, I'm not saying that that has to be the answer because I acknowledge, as Volker was saying, that there are other costs to creating those logs. But without those logs, that's the only way. As Volker even pointed out, it's too difficult to go back and figure out. You're going to go through the abuse tickets and try to connect all the dots afterwards. It's impossible. You can't do that at scale in any way. The only way at scale in a practical manner, in an efficient manner, to determine compliance is through these logs. But again, there could be other significant costs to creating those logs, so I'm not saying that has to be the ultimate answer. And I think also to address Farzaneh's and Michaela's and other concerns about the qualitative issues, again, it's through the logs. Without the logs, you can't determine whether it was proportionate or not or any of the other things. So logs is the only meaningful way, acknowledging that there are other costs which it may clutter up abuse investigations generally. But I just don't see any other way that you can meaningfully determine compliance other than those logs, especially understanding that there's not going to be any reporting from external parties. It's all going to be based on regular audits by compliance.

PAUL MCGRADY: Thanks, Mark. All right. I've got Volker and then Carlos. I'm going to hold both of you to about 30 seconds. Sorry, guys.

VOLKER GREIMANN: Yeah. Just with regard to Gabe's comments. Normally, a response is what we send back to the reporter, and we also might include in that as part of the definition of response the actual actions taken. But the actions taken usually are not logged specifically other than through the system logs that we already create automatically by taking that action.

Having to document, to list all the domain names that we might have taken down as part of the abuse complaint is quite time-consuming effort, at least for us. When I go through a reseller account and click a couple of boxes of domain names that I feel that are associated with that domain name that I'm already investigating, and take them down on that basis, then the system will create an internal command that is saved on our internal database that I will not have access to afterwards anymore.

And when I look at that domain name, I will see that the domain name was taken down at that time with that comment. But the comment is usually limited to DNS abuse detected or something like that, or phishing detected or carding detected. And that gives me a clue of why that specific domain name was taken down, but not in the context of which other domain names were taken down. In the case that I had with Mark, the only reason why I would remember why I took the other domain name down was because I remember it.

PAUL MCGRADY: All right. Thanks, Volker. I'm sorry to interrupt you. Staff, you get one minute for AOB.

FEODORA HAMZA: Thank you, Paul. This is Feodora from ICANN Org. So we will provide a summary, high-level notes, and action items from this session. However, as announced by Paul earlier, please go through the preliminary recommendations review document and the scoped impact assessment. Note anything we might have missed or is a no-go or should be improved or changed so that we can discuss during ICANN 86. That's it. Thank you, Paul.

PAUL MCGRADY: Thank you all. We'll see you soon. Safe travels.

JULIE BISLAND: Thanks everyone for joining. This meeting has concluded. Have a good rest of your day.

[END OF TRANSCRIPTION]