ICANN86 Seville | PF – GNSO: DNS Abuse Mitigation PDP 1 (3 of 4)
Wednesday, June 10, 2026 – 10:00 to 11:15 CEST

TERRI AGNEW

Hello and welcome to the DNS Abuse Mitigation PDP 3 of 4 session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning Statements of Interest.

Please observe the following guidelines to participate in the session and I will also post them in chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during the session as time permits and when directed by the chair of the session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand the floor over to Paul McGrady. Please begin.

PAUL MCGRADY

Thank you, Terri. Good morning, everybody. We are session three and moving along in all deliberate haste, but not at the cost of quality. Our menu today is brief. We are going to continue preliminary review. I'm sorry, we're going to continue review of the preliminary recommendations for Charter Questions 1 through 9.

We will do that through viewing some text for Rec 8 and 9, which we worked on yesterday. And then we have a couple of survivors on the cannot live with list that we need to go and talk about together. We've set aside a big chunk of time to get those addressed, hopefully, and wrapped up.

Before we begin, I had a request from someone in the community that I try again at explaining the difference between implementation guidance and guidance from compliance, because I think there was some confusion. So, let me do my best to try to clear that up. Implementation guidance, if we have any, which we don't have to have, but if we have any, will be underneath the recommendations.

The recommendations are adopted by Council and they go on to the Board to either be adopted or rejected. Well, we hope they're adopted by Council. There's no guarantee. But in the implementation guidance, those are where we can put some of our thoughts that really aren't high level recommendations, but things that we think the IRT, the Implementation Review Team should do or consider doing when they are implementing our recommendations.

That's Implementation Guidance, capital I, capital G. It's something that evolved in our community over time. And then we did it so much that it became a thing. That's different from a guidance document issued by compliance, right? So, when we're all done here and the IRT is done, compliance will be issuing

guidance documents to contracted parties, telling them how to comply with this so they don't get in trouble.

So, that's two different kinds of guidance. They're not the same thing. So, if you go to ICANN Compliance and you say, hey, ICANN Compliance, I'm on this working group and I wanna make sure that you guys are able to implement, or you guys are able to. consider implementation guidance and how you enforce the policy, they're going to say, we can't do that. They may not take the time to explain why they can't do that, or they may, I don't know, but they're going to say, we can't do that because they're not an IRT, they're staff, and so it's just a different thing.

So, I hope that helps clarify it. So, when we talk about implementation guidance, that's what we mean. When we talk about compliance guidance, that's what they mean. It's unfortunate they both have the word guidance in them. I hope that helps. Let us jump. Oh, there's a hand. Marc, go ahead.

MARC TRACHTENBERG Marc Trachtenberg, for the record. And so, when we have our final deliverable, our recommendations, and they go to the Council, and hopefully they're adopted and recommended to the Board, and then this goes to the IRT. Like, what do we think the IRT will produce after this? What does the final product look like?

PAUL MCGRADY

I don't know what the final product looks like for a process that hasn't happened yet, Marc, but usually it's a document that is consensus policy that then is considered to be part of the contract without necessarily amending the contract word for word in a paragraph. So, I'm going to get out of the hot seat and ask Feo to jump in and tell us what the final product will look like.

FEODORA HAMZA

This is Feodora from ICANN Org. So, I also don't know as Paul said, but implementation will be more detailed and there will be then concrete policy language based on the policy recommendation this working group developed and then they will include whatever more detailed language is going to end up in the contracts themselves.

So, there is a process there, how it's going to look like, our IRT colleagues will you let you know and we can ask them, but yeah, there will be some work to be done there. They will consider our recommendations and implementation guidance.

And just to note, implementation guidance is there to allow also for flexibility when it goes to the IRT, because sometimes there are dependencies we cannot foresee yet. And in case those cannot be implemented, the IRT has the flexibility. So, hope that helps a bit more. Thank you.

PAUL MCGRADY

Thank you. So, sometimes it's a small policy that's adopted that way. But we've seen, for example, the Paris recommendations on New gTLDs were 19 or 22 high-level statements. It's like two pages. And by the time that thing was done, the IRT had ballooned it into a 400-page applicant guidebook, right? And so, it just depends on how the IRT does.

We're narrowly scoped, so I don't envision some giant document coming out at the tail end of this. But it's one of the reasons why if there is implementation guidance that we can all get behind, we should record that so our thoughts move along with the recommendations. Anybody else have questions on that? That was a surprise to staff. I didn't tell them I was doing that. But every now and then, I like to surprise staff. It's fun. Okay, Nick.

NICK WENBAN-SMITH

Great. Thank you, Paul. It's Nick Wenban-Smith for the record. Here I am even doing the thing which I normally don't do. Welcome everybody to day three. We are in the final stages of reviewing the preliminary recommendations. We've got the last two preliminary recommendations. So, just to remind people, these are around the metrics for the policy effectiveness, which is charter question number eight here.

We haven't got the questions, so I thought it's helpful just to remind people what the charter question is. And then charter question nine is around the compliance. So, on Monday, we didn't have any preliminary text, but now we do. So, we've spent some time since

the meeting on Monday coming up with this preliminary recommendation text and rationale.

Staff sent this round to the working group list yesterday, so people should have had a chance at least to look at it and to let it percolate in terms of the discussion today. So, where we've got to is that there should be a two-year review after the implementation of the policy to see how the policy is working.

As you see here, whether it's achieving its intended purpose, can there be improvements or whether it should be quietly euthanized. So, we know this is a sort of complicated area. We talked on Monday about ideally, DNS abuse would be seen to trend downwards. But then there's other issues, DNS abuse generally could be tending upwards.

Has this policy been working or not is difficult to assess without a sort of baseline measurement. And also, abuse varies quickly. Threat actors are clever, so, abuse may move from one place to another. That doesn't mean to say that the policy isn't worthwhile and effective. So, we're looking at it with a more holistic and specific lens here.

So, are registrars actually doing their ADCs? And specifically, we've talked about the registrars, perhaps not in the room today who are not doing ADCs today, most of the registrars in the room are doing ADCs today. Are they doing their ADCs? Can ICANN Compliance assess that the ADCs are being carried out in accordance with the

policy obligation associated domains being identified and mitigated? Is there a consistency of practices across the industry?

And are there any other guidance notes or advisories that should be updated in order to assist people achieve the policy objectives here? So, as you can read from the rationale, the rationale is not part of the policy recommendations, but it's part of the context which the policy recommendation has come up with. So, abuse is dynamic, causation and correlation is difficult necessarily. Avoid the aggregate of use volume statistics, look at practical effectiveness.

As I said, I think on Monday, and I don't think I got any challenge, but there are a number of registrars who have very high concentrations of abuse, very large volumes of domain names, all from the same sort of phishing attack. Those registrars need to change their practices or frankly be put out of business.

So, if that's still happening in two years' time, then from my perspective, the policy has not worked in the way that we intended to work and when we're going through this work now. So, we expect the IRT to work on the relevant data points. We've had some discussion, I think, around the baseline measurements.

So, what we have put in here, if you look at this last sentence at the bottom of the slide, for those that don't already know this, ICANN already produces monthly DNS metrics. So, I think part of the implementation review would be to ask that team to start to include some data so that the community can see how the ADC

process has been implemented. How ADC is being carried out and try to include some of that so that people can see soon after the policy is introduced. How is ADC coming in?

And that should be included as part of the suite of metrics which are published monthly. And then when it comes to the two-year view, hopefully there won't be any surprises in terms of what's been going on. So, there should be some level of transparency at the macro level in terms of what's happening across the registrar community and the abuse mitigation statistics which are already being produced and should be enhanced to include some information around the ADC processes.

So, great. We have some questions. I was just going to ask. So, now we should have a queue of questions for some discussion on this. And I can see we have Anil, we have Thomas, Rod, and then Ching. So, Anil first, the floor is yours.

ANIL KUMAR JAIN Thank you Nick. Anil for the record. First of all, thank you very much for elaborating, and I hope that GNSO should come out the data on this policy implementation on monthly basis as you said. Now my suggestion here is about the review. Very important that the policy implementation should be reviewed on regular basis.

But what I suggest that in addition to ICANN Org to review the progress, we should have more stakeholders who should be part of the review so that in case there are issues which are related to the

stakeholders, then those are the right people to inform why issues are not -- are the policies not able to get implemented, and what are the remedial actions which are required to be taken? Thank you.

PAUL MCGRADY

Thanks, Anil. I think that's very practical. Normally, when policies are reviewed, there's an initial staff report. And so, again, and this would be not part of a formal recommendation, but it could be implementation guidance. that that staff report should take on comments from the community as part of their staff report process. They don't always do that. They often do that. And I think we should capture that thought. Thank you.

NICK WENBAN-SMITH

Great. Thank you, Paul. Thomas.

THOMAS RICKERT

Thank you so much, Nick. I think we all agree that we want this policy to be effective in getting bad actors up their game. And this is between policy and the implementation recommendations that we put into our report because I think that part of the way ICANN is implementing policy is also setting up rules on how ICANN Compliance should go about enforcing this.

So, I think we have this triangular relationship between our policy then what the Org does with it, implementing it, and also we see OCTO as one player for the review process. And I think we might

need to be a little bit more explicit in what we expect all these parties to do without being prescriptive. We don't want that to be a guide for bad guys on how to bypass the system.

But what we do know is that OCTO should be in a position with their own intelligence, as well as with information they can get from third parties, what campaigns are going on, what registrars are involved in campaigns, how many domain names are sitting with each registrar.

And they should come up with a methodology of auditing registrars based on that so that they can exactly go to the registrars and say, okay, did you receive an abuse report, did you take action with an ADC and what happened subsequently so that we don't encumber the good actors that are already doing their thing with additional auditing, but that we empower or even request with our report that ICANN structure its operation so that the bad actors are getting under more pressure.

NICK WENBAN-SMITH Excuse me. I couldn't agree more, Thomas, and you've put us native English speakers to shame with your very eloquent articulation of the exact issue. I couldn't agree more. We're trying to do this in a way which is flexible, yet gives everybody the assurances they want that the right things are going to be happening. We can't show our homework to threat actors so they

can more easily evade the policy. I don't know if you were listening to the compliance webinar a couple of weeks back.

So, ICANN Compliance gave a really helpful webinar, actually, around how they approach their work. And they certainly, from what I heard, is they can see which registrar accreditations are over-proportionate, shall we say, in the amount of abuse they've got for the volume of domains that they manage. And those are the people who they target their compliance action for, and they are more muscular and more interventionist where they can see there's obviously a problem.

Obviously, when you're going through that compliance dialogue, from what we heard, you start off with a more informal and then you end up in a more formal breach notifications when people don't change their behavior according to the policies.

So, I think what I heard from compliance is they can see very clearly where the problem registrars are, and this sort of policy will give them the tools to have those sort of conversations and to make them change their business practices to bring them up to speed with everybody else or they have to be put on notice and potentially put out of business and have their accreditations removed.

We had that, OCTO obviously look at the statistics as well. It's not just OCTO, there's a number of different metrics which they have there, but I think we heard clearly from the compliance team that they know which registrars have the over-proportionate amount of

abuse and those are the ones that are targeted first in terms of compliance and remediation.

I think I heard a very clear question from you. I heard a good articulation of the problem statement and I hope I've tried to give a bit of context to how we have tried to frame this.

THOMAS RICKERT: Nick, the question was whether this group thinks or agrees with me that we need to put some language into our report. I trust that ICANN Compliance is already doing things the way they should be doing, but the outside world will read our report and they will see it in isolation. So, if we don't connect the dots, it will look like a toothless tiger.

NICK WENBAN-SMITH: Okay, well, the text is here. Specifically, have you gotten some ideas as to how you might answer that?

PAUL MCGRADY: I can respond to that. Yeah, so thanks, Thomas. I think that's exactly right. I think it's this issue is and I put this in the chat. This issue is perfect example of implementation guidance rather than like the recommendations, which are more top line, more general. And we'll make sure that no one's objecting. No one says that we shouldn't have that. So, we'll make sure to capture that as part of

proposed implementation guidance in the draft report that is produced when we are done walking through these. So, thank you.

NICK WENBAN-SMITH Yeah, I think the policy comes first, and then the detailed implementation guidance comes second. I think the high-level policy is what we're talking about at the moment. Yeah, good conversation. Rod, I see you next in the queue.

ROD RASMUSSEN Thank you. Rod Rasmussen here. A couple of things. First, a quick point on Ying's earlier intervention. I like the concept of bringing in perspectives of people who may have a viewpoint or a view that ICANN itself doesn't, but we shouldn't create a new process, a custom process for that. A couple of points I wanted to bring up on this.

The recommendation here does a really good job of capturing, is the process being followed? It does not do a good job of capturing whether the policy is effective. What's the goal here? I believe the goal is reducing harms through malicious domain registrations. So, I would really like to see if we could capture that concept of whether the policy is doing something to improve the overall ecosystem rather than we're just following the process really well.

To that end, it's really, really hard. I've had conversations with several of the different members here as to whether, how do you measure this? I think we had on the chat a conversation on Monday

that as a result of implementing this, we could actually see abuse of domain registrations go up from a quantity perspective as the reaction of bad guys is, well, if you're going to take my domains down in batches, I'm going to just register more.

So, if that goes up, is that a failure or is it a sign of success? And how do you measure harm? Is it uptime? There's lots of different questions here. So, I think from a policy perspective, it would be good to add in something about to the extent possible, find or look for ways to measure the overall efficacy of the reduction of harm. And the implementation may be, how do you do that?

And I don't want to get into the details of that. There's been conversations about how to do that, and I think we need to have a more robust conversation about how we might capture that. The other thing about measuring that's also important to consider here is, we're trying to reduce harm and maybe we can find a way to measure that.

At the same time, I would argue that the program is effective if we don't increase significantly the amount of false positives, in other words, legitimate registrations being suspended. So, we need to capture that concept as well because we don't want this policy to harming innocent efforts as well. Thank you.

PAUL MCGRADY Thanks, Rod. Yeah, I think, again, fortunately, we have transcripts. We're going to be able to capture that. We also see some

interesting items in the chat right now, some good detail. All that will be looked at. Again, likely in an implementation guidance rather than in the policy recommendation itself, in terms of the overall goal, Rod, you're 100% right that the overall goal is a reduction in harm, right?

Hard to measure, especially because everybody's in sessions this week saying that, like, this was the pregame, and with technology changes, things are going to get weirder, not less weird. So, that's hard to measure. The one thing that we can do, like the stated goal, is to bring off the sidelines bad actor registrars that aren't doing this.

And frankly, lazy registrars that aren't doing this are not necessarily bad. Or maybe even good faith registrars who've been advised by their lawyers, you don't have to do this, so why take the risk. And so, we're trying to bring those people off the sidelines and into the game.

That's something we can measure easily, or not easily, but it's something we can measure. But we can also capture the idea that, as you said, to the extent possible, measure a reduction in harms. So, we'll grab that. So, thank you.

NICK WENBAN-SMITH Yeah, I think from my perspective, if you've got um, one abuse report and you have a registrar who has 100 domains all as part of the same overall attack, that one abuse report should be sufficient

to take down all 100. You shouldn't have to file 100 abuse reports. So, I think we should try and capture that in that if that's possible. So, the people who are not doing ADCs today should be doing them into by the by the time the policy is brought in.

And you shouldn't have to make a hundred separate reports of abuse in order to take down 100 domain names which are all part of the same coordinated phishing attack. I think that's for me in a nutshell where how we can tell if the policy is working or not. We'll try and capture that either here or through the commentary. I have Ching next in the queue.

CHING CHIAO Thank you very much. Ching here for the BC. Couple points here. Firstly, because this particular PDP work, it's just part of many PDPs down the road. So, measuring this particular ADC effectiveness probably is too narrow or too early to say that in two years whether ADC will work or not because without considering the other few, let's say the DGA, the bulk registry variation, those other PDP which hasn't been launched yet, we really don't know how overall we can reduce the abuse incidents over time.

So, that's number one. We should probably not narrowly look at this particular one and see if this work in two years. Probably we should have a broader view. That's number one. Number two is that I'm simply reading this preliminary recommendation. So, I agree what Thomas was saying about it looks to me that the working group is recommending that waiting for two years for a

review, which shouldn't be the case, as this the text here is also showing that the landscapes keep changing, keep evolving.

So, I would probably look for probably adding some of the more urgency type of wording here saying that at least a monthly report by the staff, by the compliance is definitely needed to build on the baseline. Either it's valued qualitatively or quantitatively. I would like to see some urgency wording here. And the number three is that I'm glad to see the IRT wording is added here. It's fantastic.

But I'm also a little bit concerned on the timeline to launch this ADC, put the ADC policy into the real world, let's say, after the Board approves, and then the staff will put together an implementation guidelines and those guidelines would be reviewed by IRT, big or small, we don't know. But it probably is based on the previous a couple of the IRT words seems to have the possibility of another, maybe three to six months of "delay" to actually launch the ADC policy, which the community didn't expect that you will have a further delay.

NICK WENBAN-SMITH Okay. Thanks. There's a lot of points in there. I mean, I think you made a good point around the other PDPs. There's other further work ongoing. So, I just want to remind people that this is a specific mission. This is like a covert Navy SEALs operation, a limited specific objective. We get in, we do the policy, we get out, we do other policy work.

So, we should keep our minds focused on this specific thing around the ADCs. The actual adoption of policies by the Council and then by the Board, that is not within our power, right? But what we can do is try to come up with a clear, helpful policy, thinking forwards to the implementation of that policy and trying to help people.

So, that's the first thing I'd say. The second thing, I think from the collaboration document, the two-year review seemed to be supported generally, but we can obviously change that. If you think there was support for a review after a shorter period of time, then that's within this group's collective gift to do that. Obviously, we don't want to spend too much time reviewing.

I know review is a slightly toxic term in the ICANN environment. But that's why I wanted to include this bottom sentence around we want the reporting team within ICANN to start reporting from the moment that the policy is implemented about how ADCs are being carried out.

So, we get monthly reports tracking and being able to see how that ADC process is going through so there's a bit of transparency from day one. So, that's what we did as the compromise around the timing instead of having to wait for two years of silence and then to see what the report comes up with. Paul, did you want to add anything to that?

PAUL MCGRADY

Just that it's not unusual for members of a working group to also volunteer to be on the IRT. And so, to the extent that you feel urgent about this work when we're done, I encourage you to talk to the people who sent you here to try to get them to send you to the IRT as well and bring that sense of urgency that we have to the IRT.

It's not something we can control. We can't control how fast Council moves. We can't control how fast the Board moves. We can't control how fast the IRT moves. But even though our little merry band here will be disbanded and I will be on the ICANN equivalent of a desert island, we can all still bring in our sense of urgency as working group members.

So, I think that's that. And I'm seeing a lot of really good ideas in the chat. I'm going to hand this back to Nick. Brian, we have up at Yao, has entered the queue, and I think he's going to talk about false positives, and I'm curious to hear more about that.

NICK WENBAN-SMITH

Thanks. Yeah, good conversation, and I think these conversations are very good for essentially raising the collective consciousness across the people in this area and we should use that to build on things like the implementation as Paul was saying. Brian, we have you next and then Yao.

BRIAN CIMBOLIC

Thanks, Nick. Brian Cimbolic with the registries. Just to note and I understand the desire for more regular understanding of if the

policy is working, but I don't think that the only means by which we can understand if the policy is working and being effective is a review by staff. Specifically, we've talked about the role of ICANN contractual compliance and how the Associated Domain Check necessarily has to really, one of the enforcement mechanisms, the primary enforcement mechanism is likely to be audits.

And when ICANN conducts contractual compliance audits, they always put out a report regarding those audits. So, if ICANN work to conduct an audit. around the new obligations of the Associated Domain Check, that would provide some real insight to the community around the effectiveness of the policy, separate and apart from a separate staff review. So, just pointing out that the review that's proposed here isn't going to be the community's only insight as to the effectiveness of this policy.

NICK WENBAN-SMITH Thanks, Brian. That's a good point. So, do you think we should add into the indicators of policy effectiveness? We see the five ones there. Do you think we could add in an additional one around the ICANN audit reports, if that's what's going to be helpful in terms of actual as a enforcement work?

BRIAN CIMBOLIC I think that something like that might would be good, but I think that number two already has something like that where whether

ICANN Compliance can assess compliance with the ADC obligation, I think that's that finding will be derived from the first audit results.

NICK WENBAN-SMITH: So, we could expand on number two, say for example, including audit report findings.

BRIAN CIMBOLIC: Yeah, that makes sense.

NICK WENBAN-SMITH: I'm not a fan of drafting by committee on the fly, but that language, we could easily add, I would have thought.

PAUL MCGRADY: Thanks, Paul McGrady again. And then before we send this on to Council, we're going to ask ICANN Compliance, do you have everything you need to actually enforce this? Because we don't want to go down that road. And so, if they say yes, and then two years from now they say, oh, well, we really didn't, that's going to be a bummer. So, we're going to pin our friends in on that. Thanks.

NICK WENBAN-SMITH: Good, that's a helpful intervention. Thank you. Yao.

YAO AMEVI SOSSOU

Oh, sorry. Thank you, Nick. So, I read the Premier Commission, and then I'm really worried about this thing, NCIG have been forcing the request mechanism and also like remedy all these things we haven't really look into that, but also I was wondering if we could suggest one additional bullet points about like quote lies it whether ADC related adverse impact including false positive erroneous association, reverse associations actions and resistant complaint indicate a need for additional safeguards, correct measure, or future recourse work.

I'm not suggesting that there will be a full design because mechanism at this stage right now. But I mean, evaluating whether the ADC has an effective impact then should be assessed whether this cause adverse impacts or whether those were properly addressed. For example, for in case of the false positive and erroneous association, for example, reverse mitigations, registration complaint, or case where a domain was wrongly treated as associated with an abuse activity.

So, as I said, I'm not suggesting that we have at this point a full recourse mechanism in place, but the review should measure whether the lack of clear remedy or correct path is creating additional program here.

NICK WENBAN-SMITH

No, I think that's a valuable input actually. And we did talk as the leadership team around is ICANN receiving complaints about wrongly applied ADCs leading to um server hold and domains being

taken away from people who didn't do anything wrong, the false positives.

And I think potentially part of the policy effectiveness could include, we're talking about the ICANN Compliance, are they receiving complaints about false positives, justified complaints which are upheld, that people's domains are being suspended wrongly. And I think that could easily be part of the review.

So, upheld complaints about wrongly applied domain suspension, I think is partly a way to look at that. And then we can take that language away and whether we can expand that second bullet point a bit more in the same way that Brian was talking about the audit findings, but also track record of complaints.

If there's a rising trend of complaints for people whose domains have been wrongly suspended, the false positives, then that wouldn't be a good outcome of this policy, in my view. I think that's the end of the queue there. So, I think perhaps you should move through to number nine. So, we looked at this wording on Monday, and we had quite a lot of support for the wording, so, hopefully this will be a shorter conversation.

So, registrars have to be able to demonstrate compliance. They must be able to demonstrate through records and documentation maintained in the ordinary courts of business. The trigger., whether that led to ADC being conducted. What information was reviewed? Reasonably accessible. How many associated domains

were identified? What resulting action was taken in relation to the associated domains?

That the process was reasonable and proportionate. I think this touches on Yao's last point around not having false positives as part of this process. And we were not minded, given the different registrar models, different geographic diversity languages, legal frameworks, we're not going to be too prescriptive about how that is done.

But they have to be able to evidence it to demonstrate compliance. They must have internal processes describing how they're conducting their ADCs. It should describe the steps and should take into account the applicable advisories or implementation guidance. And that internal process should be part of the process of ICANN audits. Obviously, ICANN already conducts audits.

So, this will be an additional suite of documentation and process stuff for the ICANN Compliance team to be able to assess whether or not registrars are properly conducting their obligations in line with the policy. So, that's a slight refinement of what we're looking at on Monday based on the inputs that we had.

We think it's pretty good, but we're still obviously wanting to get community input to make it even better if that's possible. And I'm very happy to take more comments or open a queue now. Marc, I see your fastest finger. Off you go.

MARC TRACHTENBERG I like this generally. I just have one question. For the trigger of the ADC, do we just mean -- oh, sorry, Marc Trachtenberg for the record. For the trigger of the ADC, we just really mean the domain name or domain names that were reported for abuse and when, right? Or should we clarify that?

NICK WENBAN-SMITH Yes, exactly. I think that's charter question number one, what triggers the obligation to conduct ADC? And we talked about the existing contractual requirement that when a registrar has actionable evidence of DNS abuse, that they have to take action. That is the trigger event is my understanding we can look back at that in the context of charter question one if that's helpful.

MARC TRACHTENBERG I guess I'm just wondering if it would be helpful to clarify here that what we really intend or what we mean is the domain name or domain names that are triggering the ADC.

NICK WENBAN-SMITH Yeah, I think that's fair. We can definitely reference back to the actual trigger requirement, which is separate. I don't want to repeat all the Charter Question 1 stuff here, but we can certainly reference back to that.

MARC TRACHTENBERG: But I think specifically timing here is important, that trigger to include the timing because that will help the metrics later of determining how long are people taking to conduct the ADC.

NICK WENBAN-SMITH: No, the point is well made and I think we've definitely heard it. I was thinking about this myself. You will see through the DNS records when an abusive domain has a server hold applied because it'll be in the timestamp when you do the RDAP check on it.

And then for associated domains, similarly, there will be timestamps on mitigation action, and that should be well auditable. You'll be able to see exactly what the time is, and certainly ICANN Compliance will have access to all the registrar records to see exactly that.

MARC TRACHTENBERG: But I think when the original triggering domain or domains is put on client hold, then when the other ones are, it's not necessarily when the report was received. I think that's the more important information that you want to probably capture, right?

Because the ADC is triggered by when you have the actionable evidence of DNS abuse. And so, when we're looking back later and we're trying to determine how this is working in practice and we want some good metrics, that seems like some important information to capture.

NICK WENBAN-SMITH I think that's a slightly different point. So, what we're talking about here is the trigger domain and then the ADC and then any follow-on action as a result of the ADC. I think what you're talking about is the abuse report, then the initial action, which triggers the stuff downstream.

MARC TRACHTENBERG I'm not talking about downstream. I'm talking about the triggering of the ADC. So, I think it's important to capture when did the registrar have the actionable evidence that triggered the ADC and then when was the ADC actually conducted? That's something that I think Compliance is going to want to be able to look at.

That's the important point, because Compliance is going to want to look at and determine, okay, was this registrar prompt in doing that, or was it a reasonable amount of time, whatever that standard is? And you can't be able to figure that out if you don't know when the trigger actually happened.

And then if the ADC was conducted, when it was conducted, that's an important delta right there for looking back at effectiveness. And that's why I think we should think about having some clarity here on that timing element.

PAUL MCGRADY Thanks, Marc. Paul McGrady, for the record. So, I think what you're saying is the first bullets that say the trigger and timestamp, the trigger with its timestamp of whatever trigger the ADC.

MARC TRACHTENBERG I don't know if it's timestamp, but that's the concept. Yeah, I don't have the exact word.

PAUL MCGRADY Because whether and when an ADC was conducted, if you might know when it was conducted, but without knowing when the trigger happened, it's a free-floating item of data that doesn't really help you correlate anything.

MARC TRACHTENBERG Right. This is not able to determine, like, was it a reasonable amount of time or was it prompt? I don't remember what the standard is, but.

PAUL MCGRADY Yeah, we understand that. And that to me is instead of demanding, 2472, you guys have stepped back and given ground on that. I think the thing that's left over from that is we still want to understand the timing, though. And so, without knowing when that ADC was first triggered, we can't know whether or not the when it was done was done in a prompt way or not. So, we'll grab that.

MARC TRACHTENBERG Right, I think that's what's contemplated in trigger. I think would be helpful to clarify.

PAUL MCGRADY Yeah, it's implied, but I think we can make it a little more direct. We'll come back when we do the next iteration of documents. We'll come back with something that tries to capture that.

NICK WENBAN-SMITH I was just thinking on the fly, but what you've said, we've tried to capture. It should be within this. If it's not explicit, it should be implicit. So, the requirement is to be prompt, right? So, we could expand the second bullet point here to see whether and when an ADC was conducted and whether that was prompt in line with the policy requirement. Is that helpful?

MARC TRACHTENBERG Not really because you can't determine prompt without knowing when your initial trigger was. If you're going to do any sort of analysis as compliance, if you're looking at it, the most critical initial thing is, what was the trigger? And then when did it actually happen? If it happened, maybe it didn't happen, right? But if it did happen, when was that? You can only know that with the two data points.

NICK WENBAN-SMITH I'm sorry if I'm being slow, but doesn't the second bullet point capture that? Or if it doesn't capture it specifically, could you specifically help us expand the second bullet point to make sure that it does capture what you want us to do.

MARC TRACHTENBERG The first bullet point is the issue, not the second point. The second bullet point is clear. The first bullet point doesn't specify that the timing is important of capturing the timing.

NICK WENBAN-SMITH Okay. Yeah, let's think about that. We have Ching, and then Brian.

CHING CHIAO Thank you, Nick. Ching from the BC. I'd like to raise a point here about how we actually use the term ADC here. So, for example, the first bullet point, very clear that the action of the trigger of the ADC means ADC. We're taking an ADC action, right? The second bullet point, we're saying that whether and when an ADC was conducted. So, the way I read this is that the registrar might only just do once, right?

So, it's triggered and it's done one time of ADC at a certain time, whether it's 24, 48, or maybe actually within the week. But in many of the cases, for example, for ourselves, it would take probably several weeks or even months to do a couple of the ADC to get a full picture of a particular ADC group.

So, this could be a multiple ADC performed, and then to get the full ADC group. So, I just want to point that out here. Thanks.

NICK WENBAN-SMITH: Thanks. Yeah, hopefully we've tried to address that through this text and the discussion. As you say, it's still not settled. But yeah, thank you. Brian, I have you next.

BRIAN CIMBOLIC: Yeah, so Brian Cimbolic with the registries. To Marc's point, I put some potential language in the chat, that the first bullet could be something like initial domain triggering the Associated Domain Check and the timing of mitigation of the initial domain.

Because to Marc's point, that's the key point, is to determine the promptness of the Associated Domain Check. The first domain was engaged in abuse. When did you act on it? And from that point, when was the Associated Domain Check conducted so that Compliance can assess whether or not it was done in a prompt manner?

NICK WENBAN SMITH: Thanks. And I can see your comment there around the initial triggering of the ADC and the timing of the mitigation of the initial domain, which is the trigger, as we know, for the ADCs here.

By the way, we have gone over time around these discussions, but I think it's not a bad thing, and the level of detail we're into, I think,

shows that there's a large convergence on the overall principles of what we're trying to do here, and it's helpful to get into some of these details, particularly when you look at the homework that we're doing ahead of time for the implementation folks. So, I have Volker, and then I think we'll close the queue there and move on to the Cannot Lives With. Volker.

VOLKER GREIMANN

Yes, thank you. And while I'm not opposed in general principle on many of the things that we are here looking at, I have a bit of a concern that this can turn into a bureaucratic monster. Even if it says that it's limited to records and documentation maintained in the ordinary business, it still says that we must be able to demonstrate certain things.

The trigger of the ADC, well, any report is that's okay, but the second part, whether or not an ADC was conducted. In many cases, this is a query of a database of various search terms that depend on the original complaint. These are never logged. I'm not sure how I would ever be able to document that other than creating new logs that currently do not exist that will take time to do and that will slow me down in conducting my abuse reviews and the ADCs themselves.

Anything that is counter to the basic principle of effectiveness in dealing with abuse is not what we're looking for, and I thought we had originally agreed on not doing that. So, I would be very

cautious in demanding extra record keeping and logging that we don't currently do.

NICK WENBAN-SMITH

We've heard your points on this before and I think we've tried to capture the spirit of that in the text here. There's records and documentation maintained in the ordinary course of business. So, we're not asking for a bureaucratic monster to be created here. Quite the opposite. We want this to be a flexible framework, but it does need to be enforceable because there are some registrars who don't do this and don't want to do it.

And so, ICANN, through its compliance and audits, needs to be able to enforce recalcitrant registrars who do not do this to make sure that they do do this going forward. So, that's the intent. I hope, because I know we heard that you already do your ADCs at the same time as you do the trigger mitigation.

So, we don't want to make it worse for the good guys. So, we are very cognizant and we try to capture that through the ordinary course of business records and documentation language in there. If you have concerns with that, then we should hash it out now.

PAUL MCGRADY

Paul McGrady again. So, Volker, it could just be as simple as your internal policy says we do our ADCs when we do our check, our abuse check, right? And then you'll know when you did the ADC, right? What we're trying to do is to get the people off the bench

who are not doing them. And there may be some registrars that they say, oh, yeah, we totally did that. But there's no record, there's no way for them to assure Compliance that they did. That's bad for them because Compliance needs to be assured.

VOLKER GREIMANN Yes, and I think we are on the same page here. We are trying to find a solution that works. I'm just not as convinced that this interpretation will be carried over into how compliance will operate these conditions. And that is my worry, because sometimes compliance is varied by the book, by the letter of the word, not by the spirit of what was intended. If we can highlight the spirit of what we mean a little bit more, then probably my concerns would be allayed. Thank you.

NCK WENBAN-SMITH I think we hear that, and it's possibly something for the guidance and advisories. I think that's where that sort of level of detail, and hopefully, assurance will come through. So, I'm going to hand over the mic now to Paul for the difficult part of the conversations. Oh, Feo.

FEODORA HAMZA Hi, this is Feodora for the record. To Volker's question, this is the preliminary recommendation, but we can add rationale to maybe explain further what the group meant, as noted by your comment.

Hope that helps. You cannot see it here, but we will add it to the document.

PAUL MCGRADY

Okay, great. We did it. We are a bit over time on this, but as I said in the chat and as Nick said, I think it was important to talk these all the way through and not rush them. They're the thing itself. And so, let's go on to the Cannot Live With and the Can Live With but would prefer the following language. So, we are going to be calling on people to talk about their cannot lives with and their can live with but prefer other language for the cannot lives with, but really for everybody. Indicate what the problem is you're trying to solve, right?

Sometimes we lose track and we start to believe that we are negotiating over specific language rather than trying to solve the problem. So, let's identify the problem. Explain how that problem is not already resolved by the updates made to the documents and the other draft recommendations or straw people or straw proposals, as it may be. Indicate whether or not you believe your proposed text is mandatory.

In other words, you won't budge. Or if you are open to it being iterated by the working group. And I'm going straight for the brass tacks, guys, if you are not open to iteration, if you're not open to problem solving, if you are absolutely demanding this, please do confirm that the group that sent you has authorized you to walk away. In other words, if you truly can't live without the language

you've proposed, that means you want no policy rather than something.

So, please let us know that, that you have been authorized to bolt. I don't think we're going to see number four. I think we'll see a number three, a lot of people who have a problem they're trying to solve and are open to iteration, but I'm just being direct with you guys about what a cannot live with means. Let's go on. The first one, Recommendation 1 notes, that the trigger based on actionable evidence.

The NPOC's suggestion is triggers should be based on has a reasonable basis to believe that other registered names may be associated with the same abusive activity, actor, or campaign. The leadership note on this one is that we have already discussed this one and the working group congealed around the trigger as it's currently described because the goal of the ADC is to determine what or more associated domain names are being used for DNS abuse.

And there was some, just not being able to understand how a registrar could have a reasonable basis to believe this without checking first. It seems intuitive to us, to leadership anyways, that you would have to intuit something. And so, while I would have considered this particular item to be long closed, the NPOC has said that they cannot live with this. So, can we have a member of the NPOC come forward and explain the problem they're trying to solve and walk us through this one.

YAO AMEVI SOSSOU

Yeah, thank you very much. This is Yao Sossou from NPOC. Yeah, I think initially, we mentioned that, especially from the NCSG perspective, that we are caring about the end user data protection and mechanism put in place to ensure that those data are not accessed by anybody because without, how can I put it, without reasonable legal authorization to have access to those data.

So, the point of having a reasonable basis is to believe that those other ADC registrar names were associated with the same abusive actor or not or a campaign. During the policy, we are of the belief that the ADC or the abusive domain name check will be conducted on like a bulk basis and there's no really mechanism place to know how we actually verify whether the ADC or the domain abuse name conducted is actually on proportionally basis implemented.

So, that's why, as we said, we could not live with that, but based on the inputs from the preliminary document work, I think at this stage, we kind of agree with what have been suggested so far. So, it's okay.

PAUL MCGRADY

Thank you. Okay, that's helpful. And I think the concept there is no free-floating ADCs, right? That there is no ADC without a trigger, right? And there is no trigger that doesn't then result in an ADC, right? So, we get that and we can put that in the rationale that

nothing in this is meant to encourage a registrar to conduct an ADC without a trigger.

Perfect. All right. So, I'm taking that one as withdrawn and iterated and that's great. Okay, thank you. Rec 1 notes, when a registrar has actionable evidence that a registered name is being used for DNS abuse pursuant to section 3.18.2 of the registrar accreditation agreement, dot, dot, dot. This one is up on the cannot live with.

I thought this was can live with, but would prefer different language. But anyways, I think the GAC's trying to be diplomatic as the GAC does. It's a room full of diplomats. Welcome to the room full of technologists and lawyers. But can a GAC member speak to this one?

GABRIEL ANDREWS

Hi, this is Gabriel Andrews for the record. So, the problem being solved here, I think, was articulated in the margin of the document for those that have read it. But for those who haven't, in the real world, we see a lot of scenarios where the bad guys will have changes in how a domain behaves over time.

And so, an example of this, maybe one of the very simplest examples is they might have a domain be routing to malware for maybe five minutes and then turn it off and route it nowhere for a day or a week and then turn it on again for five minutes. I think, Nick, when we were talking about this, you gave another example

of maybe one out of a hundred resolutions will route to a bad place and the other 99 won't.

And so, there's the potential, a real potential that a domain has a lot of evidence put forward to show that it is a maliciously registered domain being used for abuse, but for whatever reason, when the registrar's abuse team is looking at it, maybe at that instant of analysis, it isn't being used in that instant. And that's the weakness that we identify here with this language.

And we're seeking the help of the group here to come up with language that addresses the risk of the domain being well evidenced that it was used in abuse and needing that ADC to occur, or even if there is a lot of evidence points that it will imminently be used in the future for abuse and ADC should occur in a way that doesn't allow a non-helpful registrar to use as an excuse. Well, it's not resolving right this second, so therefore I'm going to do nothing. Over.

PAUL MCGRADY Thank you. I'm just going to ask you to a follow-up question. One of the concerns that we heard was on the was being used. I don't know that we talked about the pattern all that much because I think that's probably the core of it. Somebody asked, and I don't know who it was, in my head, it was Reg, but that may not be factual, what happens if it was being used four years ago for abuse,

right? So, was being used as this big idea, is there a way to iterate that language to deal with that?

GABRIEL ANDREWS

Yes, I think we can workshop this as it's already started to happen in the chat. And I will acknowledge Jothan is helpfully showing an indication to work on this. I think that we acknowledge too that we're not seeking to go past to prior registrants with this. You're trying to address the abusive malicious registrant here.

And so, if we can have the assistance, perhaps, of the registrar stakeholder constituency in coming up with language that works for them, but addresses this real scenario that we're talking about, I think that'd be very helpful. And I think there's opportunity to find that kind of consensus, because what I'm not hearing is an absolute refusal to recognize that this is a real problem.

And so, I think that we can find the right language that everyone would be helpful or agree would be helpful. And so, I'm optimistic and also agreeing with you that we had inserted this in the can live with but prefer some sort of collaboration on. Over.

PAUL MCGRADY

Thank you. And I appreciate that. So, we have a queue. So, hopefully this queue helps us solve it. We're going to go with Jothan first.

JOTHAN FRAKES

Thank you. And I encourage people to look at some of the chat dialogue on this so I don't relitigate that and I'll leave room for others. Hi, Jothan Frakes with SSAC. So, what I was mentioning here, I think the objective, as I read it, with was, is to identify as part of ADC if there's other activity that's been going on but may not be active now, using some kind of data that would be forensic signals of some activity, which is good.

And now, when you're using that data, one of the things the data sometimes just identifies a domain and it doesn't necessarily define the registrar of record of the domain at the time. So, let's say that name gets actioned and deleted, now gets re-registered at a new registrar.

You want to make sure that either you're identifying the pool of the registrant data together with other forensics in order to make sure you're not going to penalize some new registrant for the actions of some prior miscreant. So, if this was, if we can tweak this, and we're already looking at how to do that, that would be, I think, more constructive so we're not creating more harm or affecting people that we shouldn't. Thank you.

PAUL MCGRADY

Thanks. We're going to do a unique queue where we're going to let the GAC react to each thing if they want to. So, back to Gabriel.

GABRIEL ANDREWS

I think that's very helpful and constructive of feedback. And I'm seeing yeses here from my counterparts. I think that we also very much appreciate the tactic and recognizing that, yeah, this is something we can address. I think it's going to take some more time to workshop. I don't know if we necessarily need to fully do it in the moment, but I actually want to ask that question of you, Paul. Do we need to fully workshop at this moment, or can we just recognize that this is something that needs to be workshopped and take time in successive meetings to do so? What's your preferred course of action?

PAUL MCGRADY

Thanks. That's a great question. In my head, we are going to onboard everybody's helpful suggestions about how to solve this problem and then we'll iterate that in the next document rather than trying to congeal it down and figure out where the semicolons go. Or if somebody wants to draw a line in the sand and push back, this is the time to do it. Yeah. Volker.

VOLKER GREIMANN

Yes, and I agree that there's a problem because obviously for us, the abuse needs to be verifiable. And if it's not verifiable from the data that we have or from the context that's provided in the report, then that's not helpful. That's why we usually advise reporters to include everything they have on the abuse. So, if they see that this

is an intermittent pattern, then they should include that in fact in the information.

If they see that this is something that can only be seen from a mobile from Brazil, then they should include that information in the report. That is helpful for us because that allows us to measure that. Similarly, sometimes we see reports that seem to match the same pattern but are actually legitimate domains being used in an exploited service.

One very common example is domains registered for traffic arbitration or monetization, which lead to various advertisers that pay for the traffic and sometimes bad actors slip through. So, these domains are virtually undistinguishable from abusive domain names. We only detect them because we know that's the parking provider that they're pointing at.

That's usually better addressed at the parking provider than at the registrar. But there's levels and degrees of how we can mitigate that. The best advice I can give at this point is include that information in the report, and then we can deal with that and treat it appropriately. And if we see multiple domains that match the pattern, we identify that the first name was used in that way, then we can take care of all the other domains as well, even if they're not active or they haven't been weaponized yet.

GABRIEL ANDREWS

Yes, I think you're speaking to the concern. And I think also I'm hearing you say that you need to still have that level of actionable evidence, whatever it may be, and I think that we're all on the same page about that. And that might change by the circumstances as you're articulated, but I hear agreement that, yes, even if the domains themselves aren't being used, if that actionable evidence threshold has convinced you that they imminently will be, that it should still be reasonable that you conduct the ADC. Am I misrepresenting you, Volker?

PAUL MCGRADY

That all is very sensible, right? So, we're talking about the difference between a registrar having to go out and dig up the pattern versus the pattern that was alleged in the abuse report, right? And so, one I get, if it's in the abuse report and it seems to match, then that's the pattern that a registrar should look at. We don't want to create a new obligation for the registrars to become the investigation wing of ICANN. Yeah. Okay. Detective Volker just got a new title. Eberhard.

EBERHARD LISSE

Okay. Eberhard Lisse, .NA. I'm with the ccNSO, appointed member. Jothan, what you said that you want to prevent them to re-register the name, we can't do that. They go to another registrar. Never mind that my experience is these are throwaway domain names. They register them, they get demitigated, they're gone, they put

something else. I am having a little problem with the language for imminent or future use.

Remember my email of a week ago, we came about a farming domain where somebody registered government or govnaa.top, put Nampol in front and send us an email to pay a ticket. Yeah, and the website looked similar, very similar to the Nampol website. But Nampol is .gov.na. So, obviously, clearly malicious takedown. Never mind, the registrar sends me form letters whenever I ask them about more detail.

They sent me the same form letter, so I'm going to speak with somebody from Compliance. I must just find somebody to talk to about it, because I wanted to see for this group how Compliance actually works on a live example. Now, if somebody registered gov.bw, gov.fr.top, and gov.br.top, as long as there is it doesn't become to the attention of a register for a trigger, nothing needs to be done.

But as soon as one of them becomes a trigger element, then all of those should go as far as I'm concerned. I'm fully with the GAC on this one. We just need to tighten the language a little bit. I am very opposed to having punishing before the crime, so to say. But if it's obvious that this is deceptive registration and end by the same person or entity or for whatever criteria we define, and one of them is actually being used, that should be enough. There should be a minimum threshold so that we just don't leave it totally to the discretion.

PAUL MCGRADY Thank you. Yes.

MARTINA BARBERO Just to say that I think we are on the same page, Eber. Maybe it was not clear that our suggestion was just to change what is in the red. The rest is just irrational. There is no language suggestion there whatsoever. It was just to change that is being used with something around what we put in red, which, as Volker also noted, misses a DNS before abuse. So, it's really not the final language.

It was just we were trying to go from this room. If there was an agreement, then when the threshold of evidence is reached, we can act because that's what the GAC wanted to achieve. So, the problem, I think we are solving it, and I think we can maybe find the details of the language based on a suggestion from the leadership team or further discussion. But if there is no concern about the concept itself, I think we're in a good place.

EBERHARD LISSE As Greg said, we probably need to workshop the language a little bit. Or as they say in English, wordsmith it a bit.

PAUL MCGRADY Thanks. Okay, we need to get moving on this because we only have six minutes left in this session. But I think that that's right. Eberhard, I hear you. I agree entirely. Not only do we not want

Detective Volker, but we don't want Detective Volker of the pre-crime division. So, yeah, for sure. All right. So, we have Rod and then Marc, and then I think that will kill it. Then I'll take out the rest of our time and we'll have to take up the rest tomorrow. Rod.

ROD RASMUSSEN

Thanks. We discussed this in the SSAC and we definitely support the concept of getting these, the idea of these campaigns where you have obfuscation or whatever getting in the way handled in the language. I just want to point out, we don't want to conflate evidence on a trigger domain with what you end up finding in an ADC.

So, ostensibly, if you get a report of abuse happening on a domain, that actually happened at certain timestamp and that was put in. What you find in ADC may have different registration periods and that should be handled in how you do an ADC and doing that properly. So, let's make sure the language doesn't mess that up, too. Thanks.

PAUL MCGRADY

Thanks, Rod. That takes us to Marc.

MARC TRACHTENBERG

I definitely agree with the concern that the GAC identified, and this is an issue that we face all the time with how bad actors try to hide evidence of their misuse of domain names. But I think this is

actually more of an issue for the DNS abuse amendments than it is maybe for this PDP.

I mean, I guess I would argue that if the bad actor is using it intermittently, and I think maybe to Volker's point, I would point that out in my abuse report so when I look at it and I see that right at the moment, I happen to check last, there's no phishing website or there's, I don't know, whatever else is not going on at that moment, but we captured in the past from my perspective.

And I think Compliance would probably agree that is a domain name that's being used for DNS abuse. I mean, not if it's 10 years ago, but it was like two days ago and four days ago, and then not today. I would note that and try to clarify that as you want to well document and evidence your abuse complaint.

So, I think maybe this issue is better addressed there than maybe here. And we're relying on the standards of what is DNS abuse as the trigger. So, I just would put that out there.

PAUL MCGRADY All right. Thanks, Marc. Yes, to good DNS abuse reports, but I do think that the GAC's concern is real in the ADC check environment as well. So, it sounds like other than you, we have good movement towards looking at the established pattern of abuse idea.

MARC TRACHTENBERG I'm okay looking at that. I was just, I guess, saying that I'm also okay, just like leaving the language the way that it is. I guess I was

suggesting that this is a real concern, but maybe the language doesn't need to be workshopped, but I'm definitely opening into workshopping it.

PAUL MCGRADY: Terrific. So, we will iterate that language. We've only got two minutes left. So, Ching, you get 30 seconds of that. Brian, you get 30 seconds of that.

CHING CHIAO: Will do. Thank you, Paul. This is Ching from the BC. So, I guess I would generally agree with GAC's suggestion, but I found it very hard to implement the matches on the established pattern of use because it's laid out a blueprint for the ADC actors that they can just simply change the pattern of use and to avoid the ADC being checked. Thank you.

PAUL MCGRADY: Thanks, Ching. Brian, you get 33 seconds.

BRIAN CIMBOLIC: Thanks. Thanks for the three seconds, Ching. So, I think it's a bigger issue than what is happening here, to Marc's point, that is being used in DNS abuse is the language in 3.18.2. So, if we fix that problem only as it relates to associated domain checks, you're creating a sort of split regime of rules where you have a one standard for associated domain checks, one standard for 3.18.2.

So, I think we'd be better served if we had a sort of contractual compliance advisory that dealt with the exact fact pattern that the GAC is concerned about, which is real, and clarifying that that should be considered is being used for DNS abuse.

PAUL MCGRADY: Brian, good suggestion. We are out of time. Staff, AOBs or anything? Nope. See you tomorrow. Thank you, everybody. Good work today.

**[END OF TRANSCRIPTION]**