JULIE BISLAND: For the recording, this is Julie Bisland. Good morning, good afternoon, good evening, and welcome and thank you for joining the DNS Abuse Mitigation PDP 1 Webinar, taking place on Tuesday, the 8th of September, 2026. Please note the last 15 minutes of the webinar has been designated as the Q&A portion.

Questions submitted in the Q&A pod will be read aloud during that time. Please remember to state your name before speaking for the recording, and the recordings will be posted shortly after the end of the webinar on the GNSO calendar as well as on the agenda wiki page.

As a reminder, participation in ICANN, including this session, is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct. Thank you, and now I will turn it over to the DNS Abuse Mitigation PDP 1 Chair, Paul McGrady. Please begin, Paul.

PAUL MCGRADY: Good morning, everybody. Welcome to the DNSAM PDP 1 Webinar. We are going to jump right in. We've got a good amount to cover this morning. Let me talk to you about what the webinar is going to be like: one, we're going to have a nice welcome session, that's what you're in right now; two, we'll spend a few minutes on background; and then we will go into the preliminary recommendations themselves; and then we'll chat a bit about the public comment process.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

I'm going to ask my co-chair, Nick, to jump in on that and also to then handle the next session, Road to ICANN87, essentially what happens between now and ICANN87, and then I'll be back to field Q&A at the end. So, let's go ahead and get started in terms of the background of how we got here. The timeline on this one is that the GNSO Council requested an Issues Report on DNS Abuse in August of 2025.

Associated Domain Name Checks were determined as a priority topic by the community and Council for a PDP to address some aspects of DNS Abuse. And so, the timeline has been swift: December 2025, PDP initiation; working group kickoff, March 2026; and we published our Initial Report in August of 2026.

Next up is to talk about the PDP scope. The problem that we are trying to help solve is that malicious actors will register multiple related domain names. Currently, only the reported domain name must be investigated. There's no obligation to review the wider portfolio. Now, that doesn't mean that some registrars aren't doing that, a lot of good actor registrars are doing that, but not every registrar, and there's no contractual requirement.

The policy goal of the PDP is a new requirement for registrars to proactively check associated domain names linked to malicious actors and domains. And so, that's the reason why we all got together and put together and drafted the Initial Report. The deliberations that we've had, we worked on defining the triggers for associated domain name checks, the scope of the outcomes, timelines for ADCs, safeguards, documentation, and metrics.

And so, that's how we spent our time. We had some considerations along the way, including the human rights impact, global public interest impacts, impacts on consensus policies that already exist, and data privacy considerations. That is how we have been spending our time. Moving on to the next bit, this is the fun part. We actually will walk through and talk about the various recommendations that we've put together.

Recommendation 1 is the ADC trigger, the Associated Domain Names Check trigger, and this is all contained in the Preliminary Report for public comment, so these are still open for the community to weigh in on. But the working group is proposing that actionable evidence on confirmed DNS Abuse should be the ADC trigger.

Importantly, if it is a compromised domain name, that would not trigger the ADC. Just very briefly, the difference between a compromised domain name and a maliciously registered domain name is that a compromised domain name had a good-faith, non-malicious reason to be registered, but has been taken over or abused in some way by a third party.

And so, we have excluded those from the ADC trigger of Recommendation 1. And compromised domain names were excluded by the Council originally in the scope of the PDP, so no surprises there. Recommendation 2 deals with investigation. Once the trigger has been clicked, I guess, a registrar must perform a reasonable investigation in order to determine whether or not associated domains are used for DNS Abuse.

And there's all kinds of detail in the actual recommendation text for the community to look at about what reasonable investigations and all that means, but that leads us into Recommendation 3, discussion of reasonable investigation: registrars must review information reasonably accessible; a reasonable investigation must be practical and proportionate based on the circumstances.

In other words, the reasonable investigation does not require a registrar to go out and gather information that is outside of what they have in their possession, and they also do not need to boil the ocean looking under every single rock. The investigation must be practical, and we also have the word here 'proportionate'.

We had folks that were arguing strongly and succeeded for the idea that investigations should be proportionate based upon what is actually happening in and around the malicious domain name. So that's why proportionate is there. Recommendation 4 deals with determining association, how registrars do that.

Registrars must take into consideration potential indicators such as the registered name holder or account-related information, and/or technical or coordinated activity behavioral indicators. And this is a non-exhaustive list of indicators, so the idea is that there are several ways to connect these dots and different registrars are set up different ways, and so the registrars should be connecting the dots based upon these sorts of indicators.

And in the future, the reason why we have made these non-exhaustive is that things change and evolve and get better, and so if something

evolves in the future, we didn't want to have an exclusive list. We wanted the registrars to be able to evolve and to help cut back on DNS Abuse as things move along. This takes us then to Recommendation 5. Recommendation 5 are the safeguards around this process. We spent a lot of time discussing safeguards.

We have several different groups within the PDP that pushed hard and were successful in obtaining safeguards. So, Recommendation 5 sort of bakes those in: an associated domain name check must be conducted in compliance with applicable laws, including data privacy laws. In other words, you can't throw data privacy out the window just because you're doing an associated domain name check.

They also have to be conducted in compliance with ICANN's contractual requirements. This includes a non-exhaustive list of considerations such as data minimization and other things like that. So, take a good look at Recommendation 5. Again, it is to protect the registrants from overinvestigation, boiling the ocean, every rock, all that stuff.

And so, the safeguards are there to do that. In terms of Recommendation 6, that is the ADC timeline. And, again, we talked here quite a bit about whether or not we should have a specific timeframe or those kinds of things. Ultimately landed on the idea that the registrar should initiate and conduct ADCs promptly following the receipt or identification of actionable evidence of DNS Abuse.

The reason why we chose promptly is because it is the same requirement that already exists in the RAA to deal with DNS Abuse once a registrar knows about it. So, tying those two things together, rather

than creating two different timelines, two different standards, that's where we ultimately ended up. Turns out the word 'promptly' is sort of a known word and already exists in ICANN compliance documentation, so that's Recommendation 6.

Recommendation 7: measuring policy effectiveness. Policy should be measured and reviewed from time to time, and so we wanted to go ahead and bake those in. This recommendation is one for ICANN, and ICANN Org should conduct a review of the policy's effectiveness after two years. We want to give it a little bit of time to see how it does. And the focus of that should be on whether ADC obligations have been consistently performed by registrars. It's an important distinction.

We didn't want to create something that is sort of out of ICANN's control by saying whether or not this ADC has resulted in less domain name abuse. First of all, that gets into causality and causation and all kinds of other statistical problems, but secondly, we don't know, as technology continues to evolve, whether DNS Abuse will go up or DNS Abuse will go down, and it could be quite unrelated to whether or not ADC checks are.

So, what we're measuring here is not necessarily a volume issue, it's a quality issue, that whether or not the registrars are doing what they need to do. And then Recommendation 8 deals with demonstrating compliance. Registrars must be able to demonstrate compliance with the ADC requirements when the obligation is triggered by actionable evidence of DNS Abuse.

So this includes demonstrating time, information reviewed, and any other potential action taken. So those are the preliminary recommendations. We're going to go to a key takeaway page. I want to pause here for a moment and say that to me it's somewhat funny, maybe funny is the wrong word, but to see these summarized like this because it's hard for those that weren't in the working group to realize how much work and effort and discussion and compromise and creativity went into each of these to get them to the point where they are stable and out for public comment, and that they're even able to be summarized like this.

And so I just wanted to pause and thank the team for all the hard work that they did, for staff keeping us on track, and I encourage everybody who's going to consider putting in a public comment to read the entire report, not just the summary, and through that process maybe get more of a flavor of how we ended up where we ended up and what compromises were made along the way to end up with something that hopefully will help deal with the problem that's in front of us.

Moving on: key takeaways. We wanted to develop a flexible, evidence-based framework that establishes a baseline requirement for registrars, and really for all registrars, to conduct associated domain name checks when triggered. The reason why I added in the word 'all' that's not in there now is because I do want to emphasize that there are many, many of our very best registrars that have already been doing this, and they brought that experience to the table in the working group.

The goal here is to make sure that all registrars are doing this so that we can deal with as much DNS Abuse as possible in an efficient way. So,

the approach here that we wanted to take allows for flexibility to account for different operational models, technical capabilities, and business practices. So, our preliminary recommendations are designed to be demonstrable and enforceable. In other words, different registrars are set up different ways: some work through resellers, some do not work through resellers, some are corporate domain registrars, some are retail registrars.

And the goal here is to put together policy that will be flexible and account for essentially everyone and various business models, and that at the end of the day registrars will be able to demonstrate compliance, and if a registrar is not complying, that the policy will be enforceable by ICANN Compliance. And the last key takeaway: we think, we hope that the recommendations seem generally well aligned to work with existing DNS Abuse requirements.

In other words, our little plugin or module plugged into the DNS Abuse work that is already going on with registrars and ICANN Compliance is meant to fit in nicely and not to cause disruption, but to enhance things. So that's kind of where we landed on the recommendations themselves. I see some folks putting in questions into the chat.

Hopefully staff will gather those for us at Q&A time. I'm going to go ahead and turn this over to Nick, who can talk about the public comment process and then the road to ICANN87, and then I'll jump back in. Nick and I can handle Q&A together. Nick, do you mind jumping in here?

NICK WENBAN-SMITH: Thanks very much, Paul, and good job so far on highlighting the work of the group. It's a sort of a whistle-stop summary of six months of very intense work. So, I come to talk about the public comment. Obviously, it's important when you put in a public comment, if you're thinking of doing so, to read the report and understand the background and the context as to why we landed where we did, and which alternative options were considered and not put in the final recommendations, and that sort of process. A lot of work went into all of this.

Obviously, this is a GNSO PDP. There's a lot of stakeholders outside of ICANN and within different parts of ICANN who have views. It's a very high-interest topic. It's an important part of the work of the whole community to try to reduce and prevent and mitigate the effects of DNS Abuse. So, we understand that there's going to be a lot of folks interested in this and will want to have some input or at least to check that the recommendations seem to match the exam question that was presented at the beginning of the PDP.

Public comment is a really important part of, not exactly stress testing, but to make sure, I guess crowdsourced, as many eyes as possible looking at the report, looking at the recommendations. Have we missed something? Is it as good as it could be? Or perhaps are people content with where we've ended up and think it's a good process in terms of a new policy?

Those are all the sorts of inputs that we'd be looking for. The public comment lasts for 40 days. It was commenced on the 18th, so the closing date is therefore the 28th of September. Policy staff behind the scenes will be preparing a summary of what people say, and obviously

that does get published. If I move on to the next slide. There is a guide to doing the public comment.

I should say, having looked at it recently, it's helpful for those of us who are looking and reviewing the comments, which we take very seriously, that there's a little bit of structure to it. So, there is a standardized approach and structured submission form to help us analyze the comments that come in and to sort of easily pass them for approve, not approve, concerns, alternative suggestions as to wording.

I should say you don't have to answer every single question. If it's just a couple of the recommendations that you want to put input in, then that's entirely possible. You can abstain on the others or just skim through to the sections that you're interested in. There's also an open response form in the sense that you can put free text for any thoughts or additional comments that you wish the whole team to be able to see and to read, and there's no limit to obviously what you want to opine on.

Obviously, from our perspective, if they are succinct and reasoned and there's references to evidence or justification, then that is helpful and to be encouraged. The next slide, thank you. Yes. As I was saying, we really want to come up with the best policy that we can. We don't want to re-argue issues which have been argued at length during the preparation of the Initial Report.

That's not a particularly useful time, but we are open to any sort of comments or feedback which will constructively put us in a better position in terms of the policy recommendations which finally go

through to the GNSO Council and ICANN Board for approval and adoption. We want this to be a good policy, and so as many eyes as possible on it, particularly from expertise in the area of abuse from outside of ICANN, is useful.

But we don't really want to have the public comment period last longer than the time it took for the policy recommendations to be drawn up. It's been quite a quick process, and I think for those of us on the leadership side of things, we would like to produce a good set of recommendations and get them implemented in short order, and then if there are improvements over time that are needed, then we can come back and revisit them, or they can be done through guidance notes or implementation or best practice from ICANN's Compliance team.

So that is what we are looking for. I notice there have been some public comments put in already, but obviously the deadline's not for another couple of weeks. So, get through to reading the report and thinking caps on to see whether we've missed anything or there are points in the recommendations which appear to be ambiguous or could be improved. Always listening for that sort of feedback.

Looking through to the Bali meeting, the idea about the public comment timing is that we would have the public comment done in order to use the time in Bali constructively to look through the public comments and to get through to the next step in terms of adjustments required to get to the final report. I think that is all clear. You can see the running man is in September. Here we are.

We've all missed our Monday PDP meetings, so this is a sort of a regroup here, but we can see hopefully the finish line to the report is in sight. And I think now it's the Q&A. Here's the summary of the sessions which are being scheduled for the Bali meeting. That's there for the record. It'll obviously be on the meeting schedule as usual.

Assuming that there's enough public comments to go through, that's how we intend to use the time. As I said, we take the public comment process very seriously. It's important that everybody has their say, and we get as many eyes as possible on the recommendations, and we want it to be the best possible set of recommendations, no ambiguity or lack of clarity, and get them implemented. And I think now it's the Q&A.

PAUL MCGRADY: Thank you, Nick. So, I see we have one question so far in the chat. Maybe staff can help me find the others if they're there. Feo, go ahead.

FEODORA HAMZA: Thank you, Paul. This is Feodora from ICANN Org. So, we have two, I think two from the same person. If you want me, I can read out the first and you can reply, and I read out the second, then you can also answer, and then we take it from there for whoever wants to ask another one.

So, the first question is from, sorry for the pronunciation of the name, I'm doing it wrong, from Gopal Tadepalli, and the question is, “Are the variant domain names in ADC conflicting?”

PAUL MCGRADY: Thanks, Feo. So, the short answer to that is no, those are two different topics entirely, and whether or not something is a variant of another domain name is not the process that a registrar would look at. It's looking for connections to see additional domain names by the same malicious registrant, rather than looking at similarity between the domain names themselves.

And so otherwise it would be this wild investigation, because there are so many domain names out there that are similar to other domain names, and it would be a giant net. And so, yeah, those are two unrelated things and not in conflict with each other. Feo, you said there's a second one?

FEODORA HAMZA: Yes, thank you, Paul. Feodora from ICANN Org. The second question, also from Gopal Tadepalli, more of a request actually: 'Are the initial questions that made this report happen so nicely available for reference?' Back to you, Paul.

PAUL MCGRADY: Thank you. So that's another straightforward answer, which is yes, all the questions that Council fed to us are contained in the charter, and so I'll see if staff can find a link to that charter, if they haven't already, and put that into the chat before we leave here. That way, everybody can have it handy, but also I think it's referenced in the public comment information itself, so if you don't get it out of the chat today, don't worry, you'll be able to find it from the ICANN public comment page. Feo?

FEODORA HAMZA: We just received another question. I'm going to read it out if that's okay. The question is from Abdulrahman Abotaleb: 'Given the scale of more than 8 million known malicious domain registrations, what measurable reduction does the working group realistically expect this policy to achieve, and against what baseline will its effectiveness be assessed?'

PAUL MCGRADY: Thanks. I can answer that one, and that goes back to let's see if I can find the specific recommendation where we talked about Recommendation 7: measuring policy effectiveness, that the measurement is on whether or not the ADC obligations have been consistently performed by registrars, not a measurement based upon a reduction of known malicious domain names against a particular baseline.

As I mentioned when we talked about Recommendation 7, there are all kinds of factors that could make the number of malicious domain names go up or down or sideways, and while the ADC checks, we hope, have an effect on the overall volume, because of the differences between causation and other statistical issues, and also new technologies that are being introduced every day, it would be quite impossible to measure the reduction that the ADC will have with any kind of confidence that it was causation in fact.

And importantly, because new technologies are coming in, we have new domain names that are coming into the ecosystem through the New

gTLD Program, just simply having a baseline and hard number to measure against, I think, would miss the point of this policy.

The policy itself has to do with whether or not all registrars have a coherent policy that they understand and can follow, that requires all registrars, not just the ones that are doing it now, to conduct the associated domain name checks. So, I hope that's helpful. Feo?

FEODORA HAMZA: Another question, this time from Wen-Yen Tian. I'm very sorry again on the mispronunciation. The question is, 'It seems to me that this PDP imposes lots of obligation to registrars. How about other stakeholders like registries and hosting providers, etc.? Do they have a role in ADC?'

PAUL MCGRADY: Yeah, Nick, if you ever want to jump in, just jump in, but.

NICK WENBAN-SMITH: I'm very happy to speak to this. I should say by way of my background is I work for a ccTLD registry, one of the largest ones, and actually, yes, as a registry, we do conduct ADC checks. But I should say there are lots of ideas that came out of the PDP discussions, but actually our charter was quite specific that this is looking at registrars.

Registrars are obviously closest to the registrant and quite often in a good position to spot abuse of their systems at large scale, better than registries in some cases. But it was discussed that maybe registries should be doing this and maybe not just within one registrar, but inter-

registrar cooperation, which should be encouraged, but that wasn't part of our charter.

The charter was quite narrow and quite specific so that we could get through the work and produce some recommendations quickly and move on to the next topic. But I think there were a lot of discussions around why can the industry not cooperate better across registrars and between registrars and registries, and there's nothing to stop that happening from what we've done. But these are here to, I think the previous question, there's a lot of malicious registrations.

What we notice is that they're concentrated in a small number of registrars, so the idea is to introduce some standards which will make those registrars stop taking malicious registrations, make them mitigated much more quickly, and there's less opportunity for the threat actors to do that. So those guys have got to introduce new policies and procedures and raise their game or go out of business, frankly.

So that's really what the task was before us. But we had a lot of good conversation. There were Registry Stakeholder Group, from the gTLD registries, lots of registrars, lots of GAC and other people who have asking very similar sort of questions like, are there other things that can be done, and the answer is yes, there is and that sort of cooperation does happen informally, but it wasn't part of the PDP to come up with recommendations around that. But it's a really good question and something that the group did end up spending quite a lot of time talking about.

PAUL MCGRADY: Thanks, Nick. Feo?

FEODORA HAMZA: Just wanted to read out another question, this time from Francesca Lafrane, I think: 'Was there any consideration or discussion about how cybercriminals may adapt their behavior in response to this policy?'

PAUL MCGRADY: Thank you, that's a great question. We talked quite a bit actually about how the abuse ecosystem. Is that a thing? I just made it up. But the community of abusers are very smart, very wily, very creative. And that is one of the reasons why we wrote policies that are flexible.

Rather than baking in 2026 technology and baking in 2026 understandings about how all this worked, we've baked in flexible principles so that registrars could adapt to the community of abuse as they change their methods, the registrars can change their methods and draw the connections between the bad guys and their domain names a bit.

So, yes, there was quite a bit of discussion about we don't want to be outwitted by cybercriminals, and we don't want to create a policy that expires on its own because we've put in requirements that essentially become stale shortly after because cybercriminals are so creative. So, the short answer is yes, we did.

NICK WENBAN-SMITH: And I should say, this policy is supposed to be disruptive to cybercriminals. So, if they have to change their attack methods as a result of this policy, I don't see that as a failure of the policy. If we've disrupted them and forced them to find other ways to carry out abuse, then I think that's part of what our assignment has been to do.

And I think we all understand that's the nature of, it's a sort of arms race between the good guys and the bad guys, and we have to provide policies which, as Paul said, can be adjusted over time. And we also don't want to require registrars to show their inner workings so that cybercriminals can evade the efforts of registrars to prevent abuse.

PAUL MCGRADY: Any other questions? We have one from John. Feo, please read it.

FEODORA HAMZA: Thank you, Paul. John McCormick is asking, 'Was there any consideration given to a standardized reporting tool for registrars on the ADC to enable cooperation and measurement?'

PAUL MCGRADY: Thanks, John, that's a great question. That is what we would call an implementation issue. We were setting high-level policies, not baking in those kinds of things, and ICANN staff tends to run the implementation review teams. I would not be surprised if there is some sort of standardization that comes out of this, but since policy is meant to be high-level and flexible, we did not.

So, for example, this actually goes back to the prior question, which is if we put together into a policy the five things that registrars have to report, but the cybercriminal comes up with thing six, and thing three becomes irrelevant because thing six now exists, then we have a policy that is out-of-date in at least two ways.

And so, I think that those kinds of things are best left to implementation, and ICANN Org will write those in a way that allows them to be flexible and adaptable as they move forward as well. Feo, any more?

FEODORA HAMZA: Yes, I think there is another one from Abdulrahman Abotaleb: 'Now the policy excludes compromised domains from triggering an ADC. Is there yet a clearer path on what recourse does the registrant have if this distinction is made incorrectly?'

PAUL MCGRADY: That actually, and Nick, feel free to jump in, but the issue of a recourse mechanism was discussed at great length, and ultimately, we made a decision that those kinds of recourse mechanisms, whether they're for ADCs or actions following reports of DNS Abuse or other kinds of things, were outside the scope of our charter.

And we have packaged that up in a list of what we're calling really interesting or important ideas that were outside the scope of our charter. It's kind of a clunky title, but it's not quite called that, but it's called something similar.

And we're sending those back through our council liaison to the GNSO Council for further consideration if the Council decides to do that. I think it would have -- anyways, Nick, go ahead, maybe you can add some more detail.

NICK WENBAN-SMITH: Yeah, the question of compromised domains is outside of the scope of the PDP, as set out in the charter. But I think you raise an interesting point here. If I'm an innocent registrant and my domain has been compromised and is used by threat actors, then I can expect that to be flagged, and maybe I'll have some disruption to my own services if that comes up.

The ADC itself is a check to look for other indicators or clusters of domain names which have all been maliciously registered by the same group. Check itself doesn't mean that a compromised domain or any other sort of innocent domain, they may be reviewed as part of that check, but they shouldn't be acted on. The registrar should only be mitigating ones where there's actually malicious intent found behind the registration.

So, the ADC is a check by the registrar. It doesn't follow from the ADC that the registrant itself is going to be subject to any sort of sanctions, and they shouldn't be subject to sanctions if they are an innocent, bona fide registrant.

And I think in terms of the recourse, it was pointed out I think during our discussions on this, and there were some quite extensive discussions on recourse mechanisms about, well, maybe there should

be more broad recourse procedures for registrants who don't agree with the actions of their registrar.

But actually, there are some existing provisions and languages in the existing registrar agreement around registrars requiring to look seriously at complaints about how they've acted in terms of their registrants. But that is probably another topic, perhaps bigger than the work of this whole charter. Thanks.

PAUL MCGRADY: All right. More questions? Going once. Okay. Well, thank you all for joining us. I want to thank my vice chair, Nick Wenban-Smith, who has just been an incredible companion along this process, a great collaborator, smart guy, and someone who really dug in and frankly chaired some of the harder calls.

I don't know how I happened to work out my long weekends on exactly the harder calls, but Nick took a lion's share of those and got a lot of this across the finish line. I also want to thank the rest of the working group team members. If I started to name specific individuals or specific working groups, then I would end up leaving somebody out, so I don't want to do that.

But I will just say that all of you in this community sent your very best people. They worked incredibly hard. They advocated zealously, but collegially. They made compromises to get important things done, and they were able to obtain compromises from others to get important things done, and you should be incredibly proud of their hard work.

I think that this is not only a fast result, but I think it's a quality result, and it has a lot to do with the quality and the creativity of the working group members that all of you sent to this PDP, so thank you for that. And lastly and very importantly, we just got the best staff team.

This staff team was on it from the beginning, and they helped us move along fast, they helped us from getting bogged down, they created beautiful documents, and really helped keep us on track. And so, I want to say thank you to them. Thank you to the higher-ups at ICANN who supported this work by sending us your best people, and we are very thankful for them. I think that's about all I have to say. Nick, any closing words?

NICK WENBAN-SMITH: I think a massive thank you to you, Paul, because you can't thank yourself exactly, but I can. And I think you've been an important part in terms of setting the standard to keep us on track, to do this really efficiently. I should say for everybody who's not closely involved with this, it involved an hour and a half or two-hour meetings every Monday.

We have a leadership team on the Thursday. We circulate the slides in advance so that people can come sighted as to the issues at the meeting, and therefore we get some quality outputs. I don't think we could have done it any faster. And then trying to have more meetings, at one point we were going to have two meetings a week, and I think actually, paradoxically, that might have made it slower.

But it's been a heavy load. It's been a heavy lift, and Paul takes the credit for steering us I think fairly and expeditiously through. This is not

the end, but I think a lot of work has been done in short order. So, on behalf of all of the rest of us, thanks, Paul, for stepping up, and I know you have a busy schedule, and this has had to be fitted in among that, so thank you for prioritizing that work.

PAUL MCGRADY: Thank you, Nick, that's kind. I am going to hand this back to Julie, I believe, and we will go ahead and call it a day. So, Julie, go ahead.

JULIE BISLAND: Thanks so much, Paul. Everyone, thank you for joining today's webinar. It has concluded. You can disconnect your lines now. Thank you.

[END OF TRANSCRIPTION]